Introduction To
Open Source Intelligence



Written By

David Childers

www.ScenicTelevision.Com

Relaxing Entertainment For The World

Creative Common License

This body of work is released under the Attribution-ShareAlike version 3.0, Creative Common License.

The work may be freely distributed or modified for commercial or non commercial purposes.

If this work is modified, compliance with the Attribution-ShareAlike version 3.0, Creative Common License is required.

These requirements include:

- Any derivatives of this work must be attributed to David Childers and any other sources that may be used.
- Alterations, transforming, or building upon this work requires distributing the resulting work only under the same, similar or a compatible license.

For the complete legal code, please refer here:
www.creativecommons.org/licenses/by-sa/3.0/legalcode

Cover graphic
https://commons.wikimedia.org/wiki/File:2012_newspaper_reader_Santa_Cruz_Argentina_7133646327.jpg

Foreword graphic - All Is Vanity - C. Allan Gilber.
https://commons.wikimedia.org/wiki/File:Damocles-WestallPC20080120-8842A.jpg

United States Government Publications

Title 17 USC §105, Subject matter of copyright:

United States Government works, provides that "Copyright protection is not available for any work of the United States Government," defined in Title 17 USC §101, as "a work prepared by an officer or employee of the United States Government as part of that person's official duties." Therefore, only those works solely authored by US Federal Government employees are not protected by copyright in the United States.

About The Author

“My brain is only a receiver. In the Universe there is a core from which we obtain knowledge, strength, inspiration. I have not penetrated into the secrets of this core, but I know it exists.”

Nikola Tesla

The Grand Master of Digital Disaster

Published Author

Introduction To Internet Broadcasting
Amazon Publishing

Over 30 Creative Commons Computer, Technical and Internet Broadcasting Guides

Newspaper Interviews

New York Times

Internet TV: Don't Touch That Mouse!
Tim Gnatek
July 1, 2004

Lagniappe - "Something Extra for Mobile"

Mobile Gets Hoaxed
Rob Holbert
Mar 16, 2016

Cited By

Five Essays on Copyright In the Digital Era
Ville Oksanen
2009

Turre Publishing
Helsinki Finland

Open Source Developer

Developed software architecture to continuously source multimedia content to Youtube Live servers.
Scenic Television – The sights and sounds of nature on the Internet.
http://www.ScenicTelevision.com

Projects

Researched and developed documentation for Peercast P2P multimedia streaming project.
http://en.wikipedia.org/wiki/PeerCast

Researched and developed technical documentation for NSV / Winamp Television.
http://web.archive.org/web/20080601000000*/http://www.scvi.net

MidSummer Eve Webfest

A virtual International festival focusing on Digital art and Free Software that was coordinated by OrganicaDTM Design Studio.

Presentation and discussion regarding Internet multimedia content distribution.
http://web.archive.org/web/20061104230522/http://www.organicadtm.com/index.php?module=articles&func=display&catid=37&aid=61

LinkedIn Contact Information

http://www.linkedin.com/pub/david-childers/4/736/72a

Foreword

Greetings,

Information is a critical asset for any individual, organization, or business to maintain awareness and is essential for guiding financial, managerial, and operational decisions. The ability to effectively collect and analyze information requires knowledge of the fundamental principles for defining the nature of the question to be answered. It also requires knowledge of how and where to access that information.

The musical inspiration for this guide is Mr. X, by the group Ultravox from the album Vienna.

It is my sincere hope that the reader finds this guide beneficial.

David Childers
www.ScenicTelevision.com

November 2019

You must be either the servant or the master, the hammer or the anvil.
Johann Wolfgang von Goethe



Index

The Value Of Information

ATP 2-22.9
Army Techniques Publication
Open Source Intelligence
Headquarters, Department of the Army

Open Source Intelligence
Tools And Resources Handbook
Aleksandra Bielska

NATO Open Source Intelligence Handbook
North Atlantic Treaty Organization

NATO Open Source Intelligence Reader
North Atlantic Treaty Organization

Intelligence Exploitation Of The Internet
Supreme Allied Commander Atlantic
North Atlantic Treaty Organization

Open-Source Intelligence in the Czech Military:
Knowledge System And Process Design
Roman Krejci
Naval Postgraduate School

A Burning Need To Know:
The Use Of Open Source Intelligence In The Fire Service
Thomas A. Robson
Naval Postgraduate School

FM 2-22.3
Field Manual
Human Intelligence Collector Operations
Headquarters, Department of the Army

The Value Of Information

Why do we need information and why is it so important?

Information is useful as guidance for selecting a proper course of action or for making critical decisions. Individuals, organizations, businesses, and governments require accurate information to ensure that all decisions made are based on reliable data. The ability to make sound decisions is based on the quality and relevance of the information obtained.

Information also has a value, and that can be determined by how much of a benefit the data is. Did the information assist you, your organization, or business in achieving a goal? Did the information help you, your organization or company in saving money? Did the information help you, your organization, or business in raising more money?

The ability to adequately research and collect specific information requires considerable skill. The individual must have the ability to formulate specific questions and seek particular answers. These same skills are used by news reporters when they are doing an interview. The news reporter must thoroughly understand all aspects of the story that they are covering and have the ability to ask specific questions. Competitive intelligence is more than merely asking a few questions; it is the skill of researching and collecting information. This ability is based on scientific principles used by many of the intelligence services worldwide. It has become a significant function for many business operations to provide a competitive edge.

As a consumer, you look for the best prices and the best quality of goods to be purchased. That is a form of using open source Intelligence. You use newspapers, magazines, and the Internet as sources of that information. These sources of information are easily accessible and available to anyone. Organizations, businesses, and governments can use this information to become aware of financial requirements, consumer trends, market trends, or business patterns that can adversely affect an operational decision.

Publicly accessible information is readily obtainable and can be of great benefit without any negative legal ramifications. The ability to research and collect publicly available information is typically not an illegal activity. (**This depends significantly on which country you reside in and the governing laws for accessing certain information.**) Information that is retrieved from illicit sources, covered by Intellectual property rights or controlled by governmental mandates, can, however, cause severe repercussions for the person retrieving the information.

ATP 2-22.9

Open-Source Intelligence

July 2012

DISTRIBUTION RESTRICTION: Unlimited Distribution

Headquarters, Department of the Army

***ATP 2-22.9**

Army Techniques Publication
No. 2-22.9 (FMI 2-22.9)

Headquarters
Department of the Army
Washington, DC, 10 July 2012

Open-Source Intelligence

Contents

		Page
	PREFACE	**iv**
	INTRODUCTION	**v**
Chapter 1	**OPEN-SOURCE INTELLIGENCE (OSINT) FUNDAMENTALS**	**1-1**
	Definition and Terms	1-1
	Characteristics	1-1
	The Intelligence Warfighting Function	1-2
	The Intelligence Process	1-3
	The Planning Requirements and Assessing Collection Process	1-4
	The Military Decisionmaking Process	1-4
	Intelligence Preparation of the Battlefield	1-5
Chapter 2	**PLANNING AND PREPARATION OF THE OSINT MISSION**	**2-1**
	Section I – Planning OSINT Activities	**2-1**
	Define the Operational Environment	2-1
	Describe Environmental Effects on Operations	2-2
	Evaluate the Threat	2-2
	Determine Threat Courses of Action	2-2
	Section II – Preparation of OSINT Activities	**2-2**
	OSINT Exploitation	2-3
	Preparation Considerations	2-4
	Section III – Planning and Preparation Considerations	**2-7**
	Open-Source Reliability	2-7
	Open-Source Information Content Credibility	2-8
	Compliance	2-8

DISTRIBUTION RESTRICTION: Unlimited Distribution

.

*This publication supersedes FMI 2-22.9, 5 December 2006.

Operations Security 2-8
Classification 2-9
Coordination 2-9
Deception and Bias 2-9
Copyright and Intellectual Property 2-9
Linguist Requirements 2-10
Machine Foreign Language Translation Systems 2-11
Section IV – Manning the OSINT Section 2-13
OSINT Section Duties 2-13
OSINT Section at the Brigade Combat Team Level 2-13
Task Organization Considerations 2-15

Chapter 3 COLLECTING OSINT 3-1
Collecting Publicly Available Information 3-1
Research 3-3

Chapter 4 PRODUCING OSINT 4-1
Categories of Intelligence Products 4-1
Evaluate Information 4-2
Process Information 4-5
Report and Disseminate Information 4-10
Reporting and Dissemination Considerations 4-12

Appendix A LEGAL RESTRICTIONS AND REGULATORY LIMITATIONS A-1

Appendix B CYBERSPACE INTERNET AWARENESS B-1

Appendix C BASIC AND ADVANCED INTERNET SEARCH TECHNIQUES C-1

Appendix D OSINT CONTRIBUTIONS D-1

Appendix E OSINT ORGANIZATIONS E-4

Appendix F OPEN-SOURCE RESOURCES 1

GLOSSARY Glossary-1

REFERENCES References-1

INDEX Index-1

Figures

Figure 1-1. The intelligence process 1-3
Figure 2-1. Brigade combat team's OSINT section 2-14
Figure 3-1. Process for collecting publicly available information 3-2

Tables

Table 2-1. Open-source reliability ratings 2-8
Table 2-2. Open-source content credibility ratings 2-8
Table 3-1. Open-source media, components, and elements 3-5
Table 4-1. Categories of intelligence products 4-1
Table 4-2. Comparison of communication types 4-3
Table 4-3. Level, factors, and elements of media control 4-7
Table 4-4. Hierarchy of media power 4-8
Table C-1. Boolean logic operators, connectors, and delimiters C-3
Table C-2. Truncating and shortening uniform resource locators C-6
Table E-1. Open Source Academy curriculum E-5
Table F-1. Military open-source training and resources 1

Preface

ATP 2-22.9 establishes a common understanding, foundational concepts, and methods of use for Army open-source intelligence (OSINT). ATP 2-22.9 highlights the characterization of OSINT as an intelligence discipline, its interrelationship with other intelligence disciplines, and its applicability to unified land operations.

This Army techniques publication—

- Provides fundamental principles and terminology for Army units that conduct OSINT exploitation.
- Discusses tactics, techniques, and procedures (TTP) for Army units that conduct OSINT exploitation.
- Provides a catalyst for renewing and emphasizing Army awareness of the value of publicly available information and open sources.
- Establishes a common understanding of OSINT.
- Develops systematic approaches to plan, prepare, collect, and produce intelligence from publicly available information from open sources.

The target audience for this Army techniques publication is Army units at the division level and below conducting OSINT exploitation.

Defined terms are identified in the text. Definitions for which this publication is the proponent are printed in boldface. These terms and their definitions will be incorporated into the next revision of FM 1-02. For other definitions in the text, the term is italicized, and the number of the proponent publication follows the definition. Terms for which this publication is the proponent are indicated with an asterisk in the glossary.

"OSINT personnel" applies to intelligence and nonintelligence Active Army, Army National Guard/Army National Guard of the United States, and U.S. Army Reserve personnel who engage in missions involving publicly available information and open sources.

AR 381-10 defines a *U.S. person* as—

- A U.S. citizen.
- A U.S. permanent resident alien.
- An unincorporated association substantially composed of U.S. citizens or permanent resident aliens.
- A corporation or subsidiary incorporated in the United States that is not directed or controlled by a foreign government.

The following are presumed to be *non-U.S. persons*:

- A person or organization outside of the United States.
- A person not a citizen or permanent resident alien of the United States.

The use or mention of the name of any commercial or private organization or its associated trademark or services by the Army does not express or imply an endorsement of the sponsor or its products and services by the Army.

This publication applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve unless otherwise stated.

Headquarters, U.S. Army Training and Doctrine Command, is the proponent for this publication. The preparing agency is the U.S. Army Intelligence Center of Excellence (USAICoE), Fort Huachuca, AZ. Send written comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to: Commander, USAICoE, ATTN: ATZS-CDI-D (ATP 2-22.9), 550 Cibeque Street, Fort Huachuca, AZ 85613-7017.

Introduction

Since before the advent of the satellite and other advanced technological means of gathering information, military professionals have planned, prepared, collected, and produced intelligence from publicly available information and open sources to gain knowledge and understanding of foreign lands, peoples, potential threats, and armies.

Open sources possess much of the information needed to understand the physical and human factors of the operational environment of unified land operations. Physical and human factors of a given operational environment can be addressed utilizing publicly available information to satisfy information and intelligence requirements and provide increased situational awareness interrelated with the application of technical or classified resources.

The world is being reinvented by open sources. Publicly available information can be used by a variety of individuals to expand a broad spectrum of objectives. The significance and relevance of open-source intelligence (OSINT) serve as an economy of force, provide an additional leverage capability, and cue technical or classified assets to refine and validate both information and intelligence.

As an intelligence discipline, OSINT is judged by its contribution to the intelligence warfighting function in support of other warfighting functions and unified land operations.

Chapter 1

Open-Source Intelligence (OSINT) Fundamentals

Pioneer and reformative directives led to the passing of legislation that affected the U.S. intelligence community and its application of publicly available information. The National Security Act of 1992 began the reformation of the U.S. intelligence community resulting in the establishment of the Open Source Office and subsequently the Director of National Intelligence (DNI) Open Source Center (OSC) in 2005. This chapter describes the fundamentals of open-source intelligence (OSINT).

DEFINITION AND TERMS

1-1. *Open-source intelligence* is the intelligence discipline that pertains to intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence and information requirement (FM 2-0). OSINT also applies to the intelligence produced by that discipline.

1-2. OSINT is also intelligence developed from the overt collection and analysis of publicly available and open-source information not under the direct control of the U.S. Government. OSINT is derived from the systematic collection, processing, and analysis of publicly available, relevant information in response to intelligence requirements. Two important related terms are open source and publicly available information:

- **Open source** is any person or group that provides information without the expectation of privacy—the information, the relationship, or both is not protected against public disclosure. Open-source information can be publicly available but not all publicly available information is open source. Open sources refer to publicly available information medium and are not limited to physical persons.
- **Publicly available information** is data, facts, instructions, or other material published or broadcast for general public consumption; available on request to a member of the general public; lawfully seen or heard by any casual observer; or made available at a meeting open to the general public.

***Note*.** All OSINT operations conducted by intelligence personnel must comply with the legal restrictions as outlined in Executive Order (EO) 12333, DOD 5240.1-R, DODD 3115.12, JP 2-0, and AR 381-10.

1-3. OSINT collection is normally accomplished through monitoring, data-mining, and research. Open-source production supports all-source intelligence and the continuing activities of the intelligence process (generate intelligence knowledge, analyze, assess, and disseminate), as prescribed in FM 2-0. Like other intelligence disciplines, OSINT is developed based on the commander's intelligence requirements.

CHARACTERISTICS

1-4. The following characteristics address the role of OSINT in unified land operations:

- **Provides the foundation.** Open-source information provides the majority of the necessary background information on any area of operations (AO). This foundation is obtained through

open-source media components that provide worldview awareness of international events and perceptions of non-U.S. societies. This foundation is an essential part of the continuing activity of *generate intelligence knowledge*.

- **Answers requirements.** The availability, depth, and range of publicly available information enables organizations to satisfy intelligence and information requirements without the use or support of specialized human or technical means of collection.
- **Enhances collection.** Open-source research supports surveillance and reconnaissance activities by answering intelligence and information requirements. It also provides information (such as biographies, cultural information, geospatial information, and technical data) that enhances and uses more technical means of collection.
- **Enhances production.** As part of a multidiscipline intelligence effort, the use and integration of publicly available information and open sources ensure commanders have the benefit of all sources of available information to make informative decisions.

THE INTELLIGENCE WARFIGHTING FUNCTION

1-5. The intelligence warfighting function is composed of four distinct Army tactical tasks (ARTs):

- Intelligence support to force generation (ART 2.1).
- Support to situational understanding (ART 2.2).
- Perform intelligence, surveillance, and reconnaissance (ART 2.3).
- Support to targeting and information superiority (ART 2.4).

1-6. The *intelligence warfighting function* is the related tasks and systems that facilitate understanding of the operational environment, enemy, terrain, weather, and civil considerations (FM 1-02). As a continuous process, the intelligence warfighting function involves analyzing information from all sources and conducting operations to develop the situation. OSINT supports each of these ARTs.

1-7. Publicly available information is used to—

- Support situational understanding of the threat and operational environment.
- Obtain information about threat characteristics, terrain, weather, and civil considerations.
- Generate intelligence knowledge before receipt of mission to provide relevant knowledge of the operational environment.
- Rapidly provide succinct answers to satisfy the commander's intelligence requirements during intelligence overwatch.
- Develop a baseline of knowledge and understanding concerning potential threat actions or intentions within specific operational environments in support of the commander's ongoing intelligence requirements.
- Generate intelligence knowledge as the basis for Army integrating functions such as intelligence preparation of the battlefield (IPB). IPB is designed to support the staff estimate and the military decisionmaking process (MDMP). Most intelligence requirements are generated as a result of the IPB process and its interrelation with MDMP.
- Support situation development—a process for analyzing information and producing current intelligence concerning portions of the mission variables of enemy, terrain and weather, and civil considerations within the AO before and during operations (see FM 2-0). Situation development—
 - Assists the G-2/S-2 in determining threat intentions and objectives.
 - Confirms or denies courses of action (COAs).
 - Provides an estimate of threat combat effectiveness.
- Support information collection. Planning requirements and assessing collection analyzes information requirements and intelligence gaps and assists in determining which asset or combination of assets are to be used to satisfy the requirements.

1-8. For more detailed information on the intelligence warfighting function, see FM 2-0. For examples of how OSINT is used to support other intelligence disciplines and operational tasks, see appendix D.

THE INTELLIGENCE PROCESS

1-9. The intelligence process consists of four steps (plan, prepare, collect, and produce) and four continuing activities (analyze, generate intelligence knowledge, assess, and disseminate). Just as the activities of the operations process (plan, prepare, execute, and assess) overlap and recur as the mission demands, so do the steps of the intelligence process. The continuing activities occur continuously throughout the intelligence process and are guided by the commander's input.

1-10. The four continuing activities plus the commander's input drive, shape, and develop the intelligence process. The intelligence process provides a common model for intelligence professionals to use to guide their thoughts, discussions, plans, and assessments. The intelligence process results in knowledge and products about the threat, terrain and weather, and civil considerations.

1-11. OSINT enhances and supports the intelligence process and enables the operations process, as described in FM 2-0. The intelligence process enables the systematic execution of Army OSINT exploitation, as well as the integration with various organizations (such as joint, interagency, intergovernmental, and multinational). Figure 1-1 illustrates the intelligence process. (For more information on the intelligence process, see FM 2-0.)

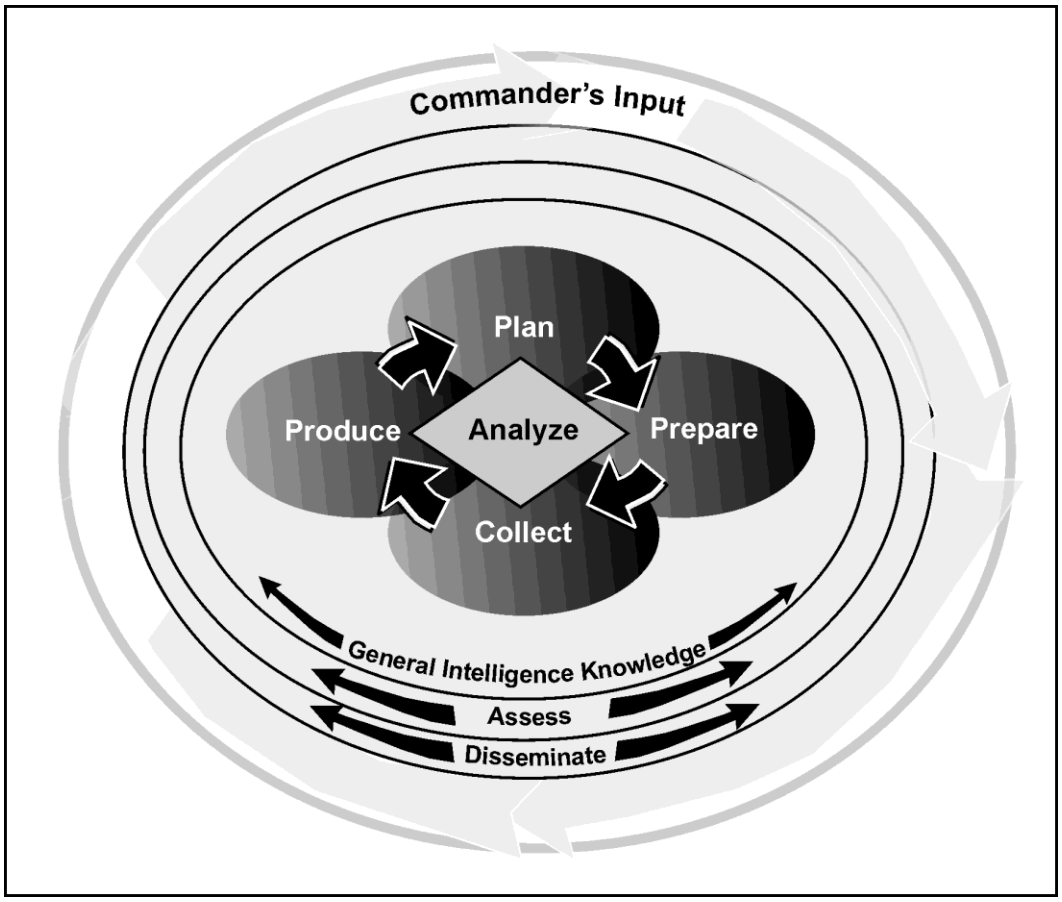


Figure 1-1. The intelligence process

THE PLANNING REQUIREMENTS AND ASSESSING COLLECTION PROCESS

1-12. Information collection informs decisionmaking for the commander and enables the application of combat power and assessment of its effects. *Information collection* is an activity that synchronizes and integrates the planning and operation of sensors, assets, as well as the processing, exploitation, and dissemination of systems in direct support of current and future operations (FM 3-55). This is an integrated intelligence and operations function. For Army forces, this activity is a combined arms operation that focuses on priority intelligence requirements (PIRs) while answering the commander's critical information requirements (CCIRs).

1-13. Information collected from multiple sources and analyzed becomes intelligence that provides answers to commanders' information requirements concerning the enemy and other adversaries, climate, weather, terrain, and population. Developing these requirements is the function of information collection:

- A *commander's critical information requirement* is an information requirement identified by the commander as being critical to facilitating timely decisionmaking. The two key elements are friendly force information requirements and priority intelligence requirements (JP 3-0).
- A *priority intelligence requirement* is an intelligence requirement, stated as a priority for intelligence support, which the commander and staff need to understand the adversary or the operational environment (JP 2-0).
- A *friendly force information requirement* is information the commander and staff need to understand the status of friendly force and supporting capabilities (JP 3-0).

1-14. The *planning requirements and assessing collection* process involves six continuous, nondiscrete activities. These activities and subordinate steps are not necessarily sequential and often overlap. The planning requirements and assessing collection process supports the staff planning and operations processes throughout unified land operations.

THE MILITARY DECISIONMAKING PROCESS

1-15. Upon receipt of the mission, commanders and staffs begin the MDMP. The *military decisionmaking process* is an iterative planning methodology that integrates the activities of the commander, staff, subordinate headquarters, and other partners to understand the situation and mission; develop and compare courses of action; decide on a course of action that best accomplishes the mission; and produce an operation plan or order for execution (FM 5-0).

1-16. During the second step of the of the MDMP, mission analysis, commanders and staffs analyze the relationships among the mission variables—mission, enemy, terrain and weather, troops and support available, time available, civil considerations (METT-TC)—seeking to gain a greater understanding of the—

- Operational environment, including enemies and civil considerations.
- Desired end state of the higher headquarters.
- Mission and how it is nested with those of the higher headquarters.
- Forces and resources available to accomplish the mission and associated tasks.

1-17. Within the MDMP, OSINT assists in enabling the planning staff to update estimates and initial assessments by using publicly available information and open sources. Major intelligence contributions to mission analysis occur because of IPB. (For more information on the MDMP, see FM 5-0.)

Note. Nonintelligence staff can also research publicly available information to prepare functional area-specific estimates, papers, briefings, plans, and orders in support of the MDMP.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

1-18. *Intelligence preparation of the battlefield* is a systematic process of analyzing and visualizing the portions of the mission variables of threat, terrain, weather, and civil considerations in a specific area of interest and for a specific mission. By applying intelligence preparation of the battlefield, commanders gain the information necessary to selectively apply and maximize operational effectiveness at critical points in time and space (FM 2-01.3).

1-19. IPB was originally designed to support the MDMP and troop leading procedures, but it can also be incorporated into other problem-solving models like design and red teaming. OSINT plays a significant and integral part during IPB in satisfying intelligence and information requirements indicated during the MDMP in support of unified land operations. The indicators that can be satisfied using OSINT during IPB include but are not limited to—

- Population.
- Propaganda.
- Commodities.
- Environment.

1-20. IPB is used primarily by commanders and staffs as a guide to evaluate specific datasets in order to gain an understanding of a defined operational environment. Prior to operations, an examination of national, multination partner, joint, and higher echelon databases is required to determine if the information requested is already available. As operations commence, new intelligence and information requirements are further identified as a result of battlefield changes. Publicly available information and open sources, when produced and properly integrated in support of the all-source intelligence effort, can be used to satisfy intelligence and information requirements. (For more information on IPB and indicators, see FM 2-01.3.)

Chapter 2

Planning and Preparation of the OSINT Mission

Directly or indirectly, publicly available information and open sources form the foundation for all intelligence when conducting operations. This foundation comes from open-source media components that provide worldview awareness of international events and perceptions of non-U.S. societies. This awareness prompts commanders to visualize a plan. Planning occurs when intelligence and information requirements are identified and means are developed as to how they will be satisfied. Effective OSINT mission planning and preparation are conducted during the Army force generation (ARFORGEN) train/ready force pool to enable the ease of transition to combat operations. (See FM 7-0 for more information on ARFORGEN.)

SECTION I – PLANNING OSINT ACTIVITIES

2-1. The *plan* step of the intelligence process consists of the activities that identify pertinent information requirements and develop the means for satisfying those requirements and meeting the commander's desired end state. As an aspect of intelligence readiness, planning for OSINT exploitation begins before a unit receives an official order or tasking as part of the *generate intelligence knowledge* continuing activity of the intelligence process.

2-2. The focus of OSINT research prior to deployment is determined and directed by the commander's guidance. Sustained and proactive open-source research using basic and advanced Internet search techniques plays a critical role in understanding AOs through foundational knowledge required for unit readiness and effective planning. Research during planning for possible missions provides insight into how nontraditional military forces, foreign military forces, and transnational threats have operated in similar AOs. Prior to deployment, organizations with dedicated OSINT missions can also be resourced to satisfy intelligence and information requirements. (See appendix E.)

2-3. After a unit receives a mission, the focus of OSINT research is further refined based on the AO in which the unit operates. OSINT supports the continuous assessment of unified land operations during planning. Effective research and planning ensure commanders receive timely, relevant, and accurate intelligence and information to accomplish assigned missions and tasks. The MDMP and IPB driven by the intelligence process frame the planning of OSINT exploitation. OSINT is integrated into planning through the four steps of the IPB process:

- Define the operational environment.
- Describe environmental effects on operations.
- Evaluate the threat.
- Determine threat COAs.

DEFINE THE OPERATIONAL ENVIRONMENT

2-4. When assessing the conditions, circumstances, and influences in the AO and area of interest, the intelligence staff examines all characteristics of the operational environment. There are preexisting publicly available inputs that can be used to identify significant variables when analyzing the terrain, weather, threat, and

civil considerations. At the end of step one of the IPB process, publicly available information and open sources can be used to support the development of the AO assessment and area of interest assessment.

DESCRIBE ENVIRONMENTAL EFFECTS ON OPERATIONS

2-5. When analyzing the environmental effects on threat and friendly operations, publicly available information and open sources can be used to describe the—

- Physical environment (terrestrial, air, maritime, space, and information domains).
- Weather.
- Civil considerations.
- Threat.

2-6. Combine the evaluation of the effects of terrain, weather, and civil considerations into a product that best suits the commander's requirements. At the end of the second step of IPB, publicly available information and open sources can be used to better inform the commander of possible threat COAs and products and assessments to support the remainder of the IPB process.

EVALUATE THE THREAT

2-7. Step three of the IPB process is to evaluate each of the significant threats in the AO. If the staff fails to determine all the threat factions involved or their capabilities or equipment, or to understand their doctrine and tactics, techniques, and procedures (TTP), as well as their history, the staff will lack the intelligence needed for planning. At the end of step three of IPB, publicly available information and open sources can provide the majority of the information required to identify threat characteristics, as well as provide possible information needed to update threat models.

DETERMINE THREAT COURSES OF ACTION

2-8. Step four of the IPB process is to identify, develop, and determine likely threat COAs that can influence accomplishment of the friendly mission. The end state of step four is to replicate the set of COAs available to the threat commander and to identify those areas and activities that, when observed, discern which COA the threat commander has chosen. At the end of step four of IPB, publicly available information and open sources can be used to determine indicators adopted by the threat commander.

SECTION II – PREPARATION OF OSINT ACTIVITIES

2-9. The reliance on classified databases has often left Soldiers uninformed and ill-prepared to capitalize on the huge reservoir of unclassified information from publicly available information and open sources, as the following quote describes:

> *OSINT was fairly new to us and once the term was understood we placed a signals intelligence analyst in charge of OSINT. At the tactical level, it seemed to be effective after the fact. There were three successful attacks against coalition forces aircraft in a specific area. We couldn't figure out the "how" and 5Ws [who, what, when, where, why] but our OSINT analyst found a downed aircraft video on the Internet that helped us identify the ingress and egress routes used during the attack that led to a "no fly" area and successful area denial missions in our area of operation.*
>
> All-Source Intelligence Analyst, Combat Aviation Brigade
> Operation Iraqi Freedom 2008-2009,

OSINT EXPLOITATION

2-10. When preparing to conduct OSINT exploitation, the areas primarily focused on are—

- Public speaking forums.
- Public documents.
- Public broadcasts.
- Internet Web sites.

PUBLIC SPEAKING FORUMS

2-11. Acquiring information at public speaking forums requires close coordination to ensure that any overt acquisition is integrated and synchronized with the information collection plan and does not violate laws prohibiting the unauthorized collecting of information for intelligence purposes. (See appendix A for further information on U.S. persons.)

2-12. Before gathering OSINT information at public speaking forums—

- Coordinate with key staff sections, such as the G-2X/S-2X, G-7/S-7, G-9/S-9, public affairs officer (PAO), and staff judge advocate (SJA), prior to conducting surveillance.
- Identify additional force protection personnel and equipment requirements.
- Identify the procedure for emplacement and recovery of audio and video processing equipment.

2-13. The operation order (OPORD), TTP, or unit standard operating procedures (SOPs) should describe how the unit that is tasked with the public speaking forum mission requests, allocates, and manages funds to purchase digital camera and audio recording equipment along with the computer hardware and software to play and store video-related data.

PUBLIC DOCUMENTS

2-14. Organizations within an AO conduct document collection missions. Once collected, documents are analyzed and the information is disseminated throughout the intelligence community. Before executing any OSINT exploitation related to collecting public documents, it is important to—

- Coordinate document collection, processing, and analysis activities across echelons.
- Identify the procedure to deploy, maintain, recover, and transfer hardcopy, analog, and digital media processing and communications equipment.
- Identify academic and commercial-off-the-shelf (COTS) information services that are already available for open-source acquisition, processing, and production.

2-15. The OPORD, TTP, or unit SOPs should describe how the unit requests, allocates, and manages funds for—

- Document collection and processing services.
- Purchasing books, dictionaries, images, maps, newspapers, periodicals, recorded audio and video items, computer hardware, digital cameras, and scanning equipment.
- The cost of subscribing to newspapers, periodicals, and other readable materials.

2-16. For more detailed information on public documents and document exploitation, see TC 2-91.8.

PUBLIC BROADCASTS

2-17. The DNI OSC collects, processes, and reports international and regional broadcasts. This enables deployed organizations to collect and process information from local broadcasts that are of command interest. Before exploiting OSINT related to public broadcasts, it is important to—

- Coordinate broadcast collection, processing, and production activities with those of the OSC.
- Identify the procedure to deploy, maintain, recover, and transfer radio and television digital media storage devices and content processing and communications systems.

- Identify Internet collection and processing resources to collect on television or radio station-specific Web casts.

2-18. The OPORD, unit SOPs, or TTP should describe how the unit tasked with public broadcast missions requests, allocates, and manages funds to purchase antenna and computer equipment, machine translation services or software, and subscribes to regional and international satellite radio and television broadcast service providers.

INTERNET WEB SITES

2-19. Information collected, processed, and produced from Internet Web sites supports unified land operations. Before exploiting OSINT related to Internet Web sites—

- Coordinate Internet collection, processing, and analysis activities across echelons.
- Identify the procedure to deploy, maintain, recover, and transfer computers and associated communications and data storage systems.
- Coordinate with G-6/S-6 for access to the INTELINK-U network or approved commercial Internet service providers that support open-source acquisition, processing, storage, and dissemination requirements.
- Coordinate with G-6/S-6 to develop a list of authorized U.S. and non-U.S. Internet Web sites for official government use, open-source research, and non-U.S. Internet Web sites restricted to selected authorized personnel engaged in OSINT exploitation.
- Identify academic and COTS information services that are already available for open-source information acquisition, processing, and production.

2-20. The OPORD, unit SOPs, or TTP should describe how the unit tasked with Internet research missions requests, allocates, and manages funds to purchase digitized documents, geospatial information, computer hardware and software applications, as well any subscriptions to academic and commercial online databases, newspapers, periodicals, and references.

PREPARATION CONSIDERATIONS

2-21. Preparing for OSINT exploitation also includes—

- Establishing an OSINT architecture.
- Prioritizing tasks and requests.
- Task-organizing assets.
- Deploying assets.
- Assessing completed operations.

ESTABLISHING AN OSINT ARCHITECTURE

2-22. OSINT contributes to establishing an intelligence architecture, specifically ART 2.2.2, *Establish Intelligence Architecture*. Establishing an intelligence architecture comprises complex and technical issues that include sensors, data flow, hardware, software, communications, communications security materials, network classification, technicians, database access, liaison officers, training, and funding. A well-defined and -designed intelligence architecture can offset or mitigate structural, organizational, or personnel limitations. This architecture provides the best possible understanding of the threat, terrain and weather, and civil considerations. An established OSINT architecture incorporates data flow, hardware, software, communications security components, and databases that include—

- **Conducting intelligence reach.** *Intelligence reach* is a process by which intelligence organizations proactively and rapidly access information from, receive support from, and conduct direct collaboration and information sharing with other units and agencies, both within and outside the area of operations, unconstrained by geographic proximity, echelon, or command (FM 2-0).
- **Developing and maintaining automated intelligence networks.** This task entails providing information systems that connect assets, units, echelons, agencies, and multinational partners for

intelligence, collaborative analysis and production, dissemination, and intelligence reach. It uses existing automated information systems, and, when necessary, creates operationally specific networks.

- **Establishing and maintaining access.** This task entails establishing, providing, and maintaining access to classified and unclassified programs, databases, networks, systems, and other Web-based collaborative environments for Army forces, joint forces, national agencies, and multinational organizations.
- **Creating and maintaining databases.** This task entails creating and maintaining unclassified and classified databases. Its purpose is to establish interoperable and collaborative environments for Army forces, joint forces, national agencies, and multinational organizations. This task facilitates intelligence analysis, reporting, production, dissemination, sustainment, and intelligence reach.

Operational and Technical Open-Source Databases

2-23. OSINT exploitation requires access to databases and Internet capabilities to facilitate processing, storage, retrieval, and exchange of publicly available information. These databases are resident on local area networks (LANs), the World Wide Web (WWW), and the Deep Web (see appendix C for additional information). To support unified land operations, OSINT personnel use evaluated and analyzed publicly available information and open sources to populate information databases such as—

- **Operational information databases**, which support the correlation of orders, requests, collection statuses, processing resources, and graphics.
- **Technical information databases**, which support collection operations and consist of unprocessed text, audio files, video files, translations, and transcripts.

Open-Source Collection Acquisition Requirement–Management System

2-24. The primary open-source requirements management operational information and technical information database is the Open-source Collection Acquisition Requirement-Management System (OSCAR-MS). OSCAR-MS is a Web-based service sponsored by the Office of the Assistant Deputy Director of National Intelligence for Open Source (ADDNI/OS) to provide the National Open Source Enterprise (NOSE) with an application for managing open-source collection requirements. OSCAR-MS links OSINT providers and consumers within the intelligence community down to the brigade combat team (BCT) level. Personnel at the BCT level access OSCAR-MS via the SECRET Internet Protocol Router Network (SIPRNET) in order to submit requests for information to the Department of the Army Intelligence Information Services (DA IIS) request for information portal. The goal of the OSCAR-MS is to automate and streamline ad hoc open-source collection requirements by—

- Providing useful metrics to understand OSINT requirements.
- Allowing the digital indexing and tagging of submitted and completed open-source products to be searchable in the Library of National Intelligence.
- Providing for local control of administrative data such as unit account management, local data tables, and local formats.
- Allowing simple and flexible formats that employ database auto-population.
- Using complete English instead of acronyms, computer codes, and other nonintuitive shortcuts.
- Allowing linkages between requirements, products, and evaluations.
- Enabling integration of open-source users for collaboration between agencies.
- Reducing requirement duplication through customers directly contributing to existing requirements.

2-25. For more detailed information on OSCAR-MS or to submit OSINT requirements, contact the U.S. Army Intelligence and Security Command (INSCOM) DA IIS at https://www.intelink.gov/sharepoint/default.aspx.

PRIORITIZING TASKS AND REQUESTS

2-26. The G-2/S-2 and G-3/S-3 staffs use commander guidance and primary intelligence requirements to complete the information collection plan. The plan is used to assign tasks to subordinate units or submit requests to supporting intelligence organizations to achieve the desired information collection objectives. Embodied in the information collection plan, these tasks describe how the unit—

- Requests collection and production support from joint, interagency, intergovernmental, and multinational organizations.
- Task-organizes and deploys organic, attached, and contracted collection, processing, and production assets.
- Conducts remote, split-based, or distributed collection, processing, and production.
- Requests and manages U.S. and non-U.S. linguists based on priority for support, mission-specific skills, knowledge requirements (such as language, dialect, and skill level), clearance level, and category.

2-27. When developing information collection tasks for subordinate units, the G-2/S-2 and G-3/S-3 staffs use the task and purpose construct for developing task statements to account for—

- *Who* is to execute the task?
- *What* is the task?
- *When* will the task begin?
- *Where* will the task occur?

TASK-ORGANIZING ASSETS

2-28. With the exception of the Asian Studies Detachment (ASD) that maintains an organic table of distribution and allowances (TDA) with the government of Japan in support of U.S. Pacific Command (USPACOM), the Army does not have a TDA or base table of organization and equipment for OSINT personnel or units when preparing to conduct OSINT exploitation.

DEPLOYING ASSETS

2-29. Deployment of publicly available assets—

- Supports the scheme of maneuver.
- Supports the commander's intent.
- Complies with unit SOPs.

2-30. The deployment of assets generally requires a secure position, with network connectivity to the Internet, in proximity to supporting sustainment, protection, and communications resources.

ASSESSING COMPLETED OPERATIONS

2-31. Typical guidelines used to assess operations are—

- Monitoring operations.
- Correlating and screening reports.
- Disseminating and providing a feedback mechanism.
- Cueing.

2-32. See paragraph 2-67 for an explanation of these guidelines.

SECTION III – PLANNING AND PREPARATION CONSIDERATIONS

2-33. Planning and preparation considerations when planning for OSINT exploitation include—

- Open-source reliability.
- Open-source information content credibility.
- Compliance.
- Operations security (OPSEC).
- Classification.
- Coordination.
- Deception and bias.
- Copyright and intellectual property.
- Linguist requirements.
- Machine foreign language translation (MFLT) systems.

OPEN-SOURCE RELIABILITY

2-34. The types of sources used to evaluate information are—

- Primary sources.
- Secondary sources.

2-35. A *primary source* refers to a document or physical object that was written or created during the time under study. These sources are present during an experience or time period and offer an inside view of a particular event. Primary sources—

- Are generally categorized by content.
- Is either public or private.
- Is also referred to as an original source or evidence.
- In fact, are usually fragmentary, ambiguous, and difficult to analyze. The information contained in primary sources is also subject to obsolete meanings of familiar words.

2-36. Some types of primary sources include—

- Original documents (excerpts or translations) such as diaries, constitutions, research journals, speeches, manuscripts, letters, oral interviews, news film footage, autobiographies, and official records.
- Creative works such as poetry, drama, novels, music, and art.
- Relics or artifacts such as pottery, furniture, clothing, artifacts, and buildings.
- Personal narratives and memoirs.
- Person of direct knowledge.

2-37. A *secondary source* interprets, analyzes, cites, and builds upon primary sources. Secondary sources may contain pictures, quotes, or graphics from primary sources. Some types of secondary sources include publications such as—

- Journals that interpret findings.
- Textbooks.
- Magazine articles.
- Commentaries.
- Histories.
- Criticisms.
- Encyclopedias.

Note. Primary and secondary sources are oftentimes difficult to distinguish as both are subjective in nature. Primary sources are not necessarily more of an authority or better than secondary sources. For any source, primary or secondary, it is important for OSINT personnel to evaluate the report for deception and bias.

2-38. Open-source reliability ratings range from **A** (reliable) to **F** (cannot be judged) as shown in table 2-1. A first-time source used in the creation of OSINT is given a source rating of **F**. An **F** rating does not mean the source is unreliable, but OSINT personnel have no previous experience with the source upon which to base a determination.

Table 2-1. Open-source reliability ratings

A	***Reliable***	**No doubt** of authenticity, trustworthiness, or competency; has a history of complete reliability.
B	***Usually reliable***	**Minor doubt** about authenticity, trustworthiness, or competency; has a history of valid information most of the time.
C	***Fairly reliable***	**Doubt** of authenticity, trustworthiness, or competency, but has provided valid information in the past.
D	***Not usually reliable***	**Significant doubt** about authenticity, trustworthiness, or competency, but has provided valid information in the past.
E	***Unreliable***	**Lacking** authenticity, trustworthiness, and competency; history of invalid information.
F	***Cannot be judged***	**No basis** exists for evaluating the reliability of the source.

OPEN-SOURCE INFORMATION CONTENT CREDIBILITY

2-39. Similar to open-source reliability, credibility ratings range from **one** (confirmed) to **eight** (cannot be judged) as shown in table 2-2. If the information is received from a first-time source, it is given a rating of **eight** and, like the reliability ratings scale, does not mean the information is not credible but that OSINT personnel have no means to verify the information.

Table 2-2. Open-source content credibility ratings

1	***Confirmed***	**Confirmed** by other independent sources; logical in itself; consistent with other information on the subject.
2	***Probably true***	**Not confirmed**; logical in itself; consistent with other information on the subject.
3	***Possibly true***	**Not confirmed**; reasonably logical in itself; agrees with some other information on the subject.
4	***Doubtfully true***	**Not confirmed**; possible but not logical; no other information on the subject.
5	***Improbable***	**Not confirmed**; not logical in itself; contradicted by other information on the subject.
6	***Misinformation***	**Unintentionally false**; not logical in itself; contradicted by other information on the subject; confirmed by other independent sources.
7	***Deception***	**Deliberately false**; contradicted by other information on the subject; confirmed by other independent sources.
8	***Cannot be judged***	**No basis** exists for evaluating the validity of the information.

COMPLIANCE

2-40. In accordance with EO 12333, DOD 5240.1-R, and AR 381-10, procedure 2, Army intelligence activities may collect publicly available information on U.S. persons only when it is necessary to fulfill an assigned function. (For more information on intelligence oversight, see appendix A.)

OPERATIONS SECURITY

2-41. OSINT could unintentionally provide present and future indicators of U.S. military operations. Information generally available to the public can reveal the existence of, and sometimes details about classified or sensitive information that can be used to neutralize or exploit military operations. Intelligence organizations

must determine the level of contact with open sources and the collection or acquisition technique that could affect Army operations.

CLASSIFICATION

2-42. AR 380-5 states that intelligence producers "must be wary of applying so much security that they are unable to provide a useful product to consumers." This is an appropriate warning for OSINT personnel where concern for OPSEC can undermine the ability to disseminate inherently unclassified information. Examples of unclassified information being over-classified are—

- Reported information found in a foreign newspaper.
- Message from a foreign official attending an international conference.

2-43. AR 380-5 directs that Army personnel will not apply classification or other security markings to an article or portion of an article that has appeared in a newspaper, magazine, or other public medium. Final analysis of OSINT may require additional restrictions and be deemed *controlled unclassified information* or *sensitive but unclassified information*.

COORDINATION

2-44. During planning, the G-2/S-2 and G-3/S-3 staff must ensure that OSINT missions and tasks are synchronized with the scheme of maneuver. Acquiring open-source information may compromise the operations of other intelligence disciplines or tactical units. Open-source acquisition that is not synchronized may also result in the tasking of multiple assets and the improper utilization of forces and equipment, adversely affecting the ability of nonintelligence organizations, such as civil affairs, military police, and public affairs, to accomplish assigned missions and tasks. Conversely, overt contact with an open source by nonintelligence organizations can compromise OSINT missions and tasks and lead to the loss of intelligence.

DECEPTION AND BIAS

2-45. Deception and bias is a concern in OSINT exploitation. OSINT exploitation does not normally acquire information by direct observation of activities and conditions within the AO. OSINT exploitation relies mainly on secondary sources to acquire and disseminate information. Secondary sources, such as government press offices, commercial news organizations, and nongovernmental organizations spokespersons, can intentionally or unintentionally add, delete, modify, or otherwise filter the information made to the general public. These sources may also convey one message in English with the intent to sway U.S. or international perspectives and a different non-English message for local populace consumption. It is important to know the background of open sources and the purpose of the public information in order to distinguish objectives, factual information, identify bias, or highlight deception efforts against the reader and the overall operation.

COPYRIGHT AND INTELLECTUAL PROPERTY

2-46. *Copyright* is a form of protection, for published and unpublished works, provided by Title 17, United States Code (USC), to authors of "original works of authorship," including literary, dramatic, musical, and artistic works. Intellectual property is considered any creation of the mind and includes, but is not limited to—

- Musical works and compositions.
- Artistic displays.
- Discoveries.
- Inventions.
- Words or phrases.
- Symbols and designs.

2-47. It is illegal to violate the rights provided by the copyright law to the owner of copyright. One major limitation is the doctrine of fair use, which is given a statutory basis in Section 107 of the 1976 Copyright Act. According to the U.S. Copyright Office, "fair use" of a copyrighted work for purposes such as criticism, comment, news reporting, teaching, scholarship, or research is not an infringement of copyright. The four factors in determining fair use are the—

- Purpose and character of the use.
- Nature of the copyrighted work.
- Amount and substantiality of the portion used in relation to the copyrighted work as a whole.
- Effect of the use upon the potential market for or value of the copyrighted work.

2-48. AR 27-60 prescribes policies and procedures for the acquisition, protection, transfer, patent usage, copyrights, and trademarks of intellectual property. Army policy recognizes the rights of copyright owners consistent with Army missions and worldwide commitments. OSINT personnel will not produce or distribute copyrighted works without the permission of the copyright owner unless such use is authorized under U.S. copyright law. There is also a requirement for OSINT personnel to forward to the Service SJA for approval and waiver of notice to the copyright holder, if necessary, for OPSEC. (For more information on copyright laws and applicability, see the International Copyright Relations of the United States at http://www.copyright.gov or the local SJA office.)

LINGUIST REQUIREMENTS

2-49. The ability to gather and analyze foreign materials is critical in OSINT exploitation. The effective use and employment of linguists, both civilian and military, facilitates this activity. The areas of the highest criticality of required foreign language skills and knowledge proficiency are—

- **Transcription.** Both listening and writing proficiency in the source language are essential for an accurate transcript. A transcript is extremely important when English language skills of the OSINT personnel are inadequate for authoritative or direct translation from audio or video into English text.
- **Translation.** Bilingual competence is a prerequisite for translations. Linguists must be able to—
 - Read and comprehend the source language.
 - Write comprehensibly in English.
 - Choose the equivalent expression in English that fully conveys and best matches the meaning intended in the source language.
- **Interpretation.** Bilingual competence is a prerequisite for interpretation. Linguists must be able to—
 - Hear and comprehend the source language.
 - Speak comprehensibly in English.
 - Choose the equivalent expression in English that fully conveys and best matches the meaning intended in the source language.

Note. Interpretation is a specific skill in which not all linguists are trained.

2-50. To effectively plan and employ linguists, commanders and staffs must understand the Army linguist proficiency evaluation system. Evaluation and reevalution of linguist proficiency is covered in detail in AR 11-6, chapter 5. Language testing is required for all Army personnel, in a language-dependent military occupational specialty (MOS) or Army occupational code (AOC), who have received foreign language training. Other Army personnel who have knowledge of a foreign language are encouraged to take the proficiency test and may work as linguists.

2-51. The Army uses the Defense Language Proficiency Test (DLPT) to measure the proficiency level in a specific language. The DLPT is an indication of foreign language capability, but it is not the definitive evaluation of an individual's ability to perform linguist support.

2-52. The Army uses Interagency Language Roundtable (ILR) descriptions of the proficiency levels for the skills of speaking, listening, reading, and writing a foreign language. Detailed descriptions of these levels are available at http://www.govtilr.org. The plus-level designators, shown as a "+" symbol, are used to designate when a linguist is above a base level, but not yet to the capability of the next level. The six base levels of proficiency as established by the DLPT are—

- **Level 0 (no proficiency).** The Soldier has no functional foreign language ability. Level 0+ is the minimum standard for special-forces personnel and indicates a memorized proficiency only.
- **Level 1 (elementary proficiency).** The Soldier has limited control of the foreign language skill area to meet limited practical needs and elementary foreign language requirements.
- **Level 2 (limited working proficiency).** The linguist is sufficiently skilled to be able to satisfy routine foreign language demands and limited work requirements.
- **Level 3 (general professional proficiency).** The linguist is capable of performing most general, technical, formal, and informal foreign language tasks on a practical, social, and professional level.
- **Level 4 (advanced professional proficiency).** The linguist is capable of performing advanced professional foreign language tasks fluently and accurately on all levels.
- **Level 5 (functionally native proficiency).** The linguist is functionally equivalent to an articulate and well-educated native in all foreign language skills; the linguist reflects the cultural standards of the country where the foreign language is natively spoken.

2-53. The above proficiency base levels designate proficiency in any of the four language skills—listening, reading, speaking, and writing. The DLPT only evaluates reading and listening skills (for example, 2+/3, or 3/1+). Currently, these tests do not evaluate linguists above the 3-proficiency level. The current Army standard to be considered a qualified linguist is a level 2. Oral proficiency interviews evaluate speaking proficiency and may be used to provide a listening score. These interviews may provide an evaluation all the way up to the 5-proficiency level.

2-54. Along with proficiency and fluency, OSINT personnel must consider the biases and cultural backgrounds of civilian interpreters when analyzing non-English open-source information. When planning to utilize linguists, commanders must identify requirements by category. Linguist screening categories are—

- **Category I.** Linguists must at least have advanced professional proficiency in the target language, a level 4 as measured by the ILR and general working proficiency (ILR 2+) in English. They may be locally hired or from a region outside the AO. They do not require a security clearance.
- **Category II.** Linguists are U.S. citizens granted access to a Secret clearance by the designated U.S. Government personnel security authority. They must at least have advanced professional proficiency in the target language (ILR 4) and general working proficiency (ILR 2+) in English.
- **Category III.** Linguists are U.S. citizens granted Top Secret (TS)/Sensitive Compartmented Information (SCI) or an interim TS/SCI clearance by the designated U.S. Government personnel security authority. They must meet a minimum of ILR 3 in both the target language and English.

MACHINE FOREIGN LANGUAGE TRANSLATION SYSTEMS

2-55. Developing a reliable and proficient linguist requires a great deal of time, both for training and gaining experience. This extended timeline often results in shortages of linguist personnel. To fill personnel vacancies throughout Army units and to meet language requirements and demands, MFLT systems are used. When employed properly, MFLT systems can provide an increased capability for translation in support of unified land operations.

2-56. Reliable MFLT capability exists to translate media broadcasts into English and there is readily available software to translate Internet sources into English as well. There are limited speech-to-speech (S2S) capabilities in use.

FOREIGN MEDIA MONITORING

2-57. Media monitoring systems like the BBN Broadcast Monitoring System™ (BMS™) create a continuous searchable archive of international television broadcasts. These systems automatically transcribe the real-time audio stream and translate it into English. Both the transcript and translation are searchable and synchronized to the video, providing powerful capabilities for effective retrieval and precise playback of the video based on its speech content. With this system, intelligence analysts can sift through vast collections of news content in other languages quickly and efficiently.

2-58. These systems provide real-time transcription and translation of broadcast television news, allowing English speakers to rapidly triage non-English television content, be alerted when new content that matches a profile is captured by the system, and work closely with human linguists and cultural experts to create actionable high-quality translations of extracted content.

2-59. The interface allows users to quickly search for specific spoken content in the video archive through keyword queries in English or the source language. Search terms are highlighted in the results, which show an image thumbnail, the transcript segment in the original language, and an English translation. Clicking on a result begins playback of the segment.

2-60. Users interact with the system from any personal computer (PC) or laptop via a common high-speed Internet connection. The only required client software is Microsoft® Internet Explorer and Windows Media® Player.

2-61. The BBN BMS™ continuously captures, encodes, analyzes, and stores live video streams in an automatically maintained, dynamic cache containing 30 days of recorded audio or video. As the video plays back, the system highlights the spoken words in both the original language and the translation. The transcript is enriched by highlighting the names of people, locations, and organizations, and by separating the speakers in the audio file. Users can jump to any point in the cache and begin playback.

2-62. Users can extract video segments or still photos for sharing, presentation, and collaboration. Demonstration compact discs (CDs) contain extracted segments that preserve the highlighting and synchronization of video, transcript, and translation during playback.

2-63. The BBN BMS™ currently translates—

- Modern Standard Arabic.
- Mandarin Chinese.
- Western Hemisphere Spanish.
- Persian Farsi.
- North American English.
- United Kingdom English.
- French.
- Bahasa Indonesian.
- Hindi.
- Urdu.

2-64. The BBN BMS™ does not require any hardware setup, software installation, or onsite administration or maintenance by the customer.

SPEECH-TO-SPEECH

2-65. Army and Marine units continue to attempt to integrate available COTS S2S translation devices into predeployment training and military operations while deployed. The primary tactical use for these devices has been language translation within security operations conducted in and among a general population of non-English speaking people.

SECTION IV – MANNING THE OSINT SECTION

2-66. OSINT personnel that comprise the OSINT section within the intelligence staff section can consist of both intelligence and nonintelligence individuals with the technical competence, creativity, forethought, cultural knowledge, and social awareness to exploit open sources effectively. The designation of OSINT personnel to satisfy requirements, missions, and tasks is generally identified by commanders and task-organized through organic assets (intelligence personnel, nonintelligence personnel, U.S. and non-U.S. contractor personnel, or linguists) in support of unified land operations.

OSINT SECTION DUTIES

2-67. The duties of the OSINT section are to—

- **Monitor operations.** This ensures responsiveness to the current situation and to anticipate future acquisition, processing, reporting, and synchronization requirements.
- **Correlate reports.** Reports (written, verbally, or graphically) should correlate classified reports through OSINT validation.
- **Screen reports.** Information is screened in accordance with the CCIRs and commander's guidance to ensure that pertinent and relevant information is not overlooked and the information is reduced to a workable size. Screening should encompass the elements of timeliness, completeness, and relevance to satisfy intelligence requirements.
- **Disseminate intelligence and information.** Satisfied OSINT requirements are disseminated to customers in the form of useable products and reports.
- **Cue.** Effective cueing by OSINT to more technical information collection assets, such as human intelligence (HUMINT) and counterintelligence (CI) improves the overall information collection effort by keeping organizations abreast of emerging unclassified information and opportunities as well as enabling the use of a multidiscipline approach to confirm or deny information by another information source, collection organization, or production activity.
- **Provide feedback.** An established feedback mechanism is required to the supported commander or customer on the status of intelligence and information requirements.

OSINT SECTION AT THE BRIGADE COMBAT TEAM LEVEL

2-68. Each combatant command may have a task-organized OSINT cell or section to some varying degree in scope and personnel. At the tactical level of operations, it is commonplace for commanders to create OSINT cells from organic intelligence personnel to satisfy intelligence requirements.

2-69. The following quote illustrates how task organization of organic personnel within the common ground station (CGS) can assist in satisfying intelligence and information requirements using the Nonsecure Internet Protocol Routing Network (NIPRNET) and various electronic devices, such as an amplitude modulation and frequency modulation (AM/FM) radio, video cassette recorder (VCR), and digital video disc (DVD) player, to ensure the success of their BCT to perform information collection at the tactical operations center (TOC):

With their CGS team, four to five interpreters, and a steady flow of radio, television, and newspaper reports, the open-source intelligence team produced a daily rollup with analysis. Their office consisted of one television with local and international cable, one laptop connected to the NIPRNET, AM/FM radio, and the daily newspaper. Also, the team acquired a VCR and DVD player to study confiscated propaganda and other media. They understand the importance of local reporting to the success of the BCT campaign and have made it a point to conduct thorough research on topics of local importance. Their product was studied and further analyzed by the (information collection) analysis team at the BCT TOC prior to submission to the BCT S-2 and dissemination to battalions or division.

Military Intelligence Company Commander, 3ID,
Operation Iraqi Freedom 2004—2005

2-70. As displayed in figure 2-1, personnel comprising the OSINT section at the BCT level include—

- Section leader.
- Requirements manager.
- Situation development analyst.
- Target development analyst.

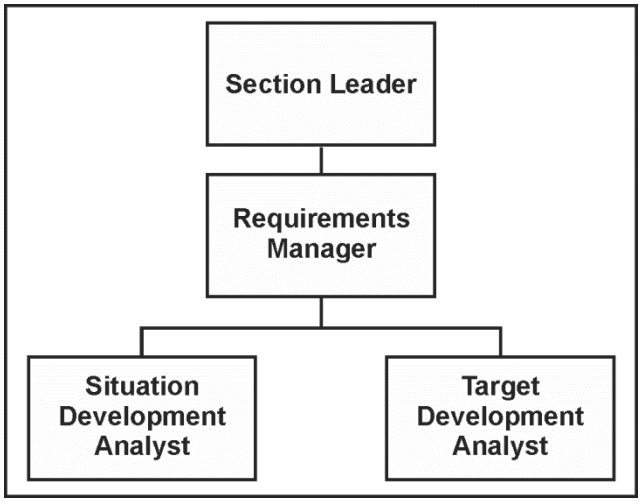


Figure 2-1. Brigade combat team's OSINT section

SECTION LEADER

2-71. The section leader—

- Is the primary liaison and coordinator with the BCT S-2.
- Provides supervisory and managerial capacity oversight.
- Sets the priority of tasks.
- Monitors ongoing intelligence support required by the BCT S-2.
- Ensures that all OSINT products are included in the planning for current and future operations.

REQUIREMENTS MANAGER

2-72. The requirements manager—

- Ensures that situation development and target development support the overall efforts of the section.
- Verifies the availability of collection assets.
- Performs quality control for situation development and target development products.
- Supervises the receipt, analysis, and dissemination of OSINT products.

SITUATION DEVELOPMENT ANALYST

2-73. The situation development analyst—

- Monitors publicly available information and open sources in order to ensure the most accurate common operational picture.
- Analyzes information and produces current intelligence about the operational environment, enemy, terrain, and civil considerations before and during operations.
- Refines information received on threat intentions, objectives, combat effectiveness, and potential missions.
- Confirms or denies threat COAs based on publicly available indicators.
- Provides information to better understand the local population in areas that include, but are not limited to—
 - Tribal affiliations.
 - Political beliefs.
 - Religious tenets.
 - Key leaders.
 - Support groups.
 - Income sources.

TARGET DEVELOPMENT ANALYST

2-74. The target development analyst—

- Identifies the components, elements, and characteristics of specific targets, both lethal and nonlethal.
- Identifies civil and other non-target considerations within the AO.
- Provides publicly available information on threat capabilities and limitations.

TASK ORGANIZATION CONSIDERATIONS

2-75. When task-organizing the OSINT section to satisfy intelligence and information requirements, units must consider—

- Mission command.
- Acquisition.
- Collecting and processing.
- Production.
- Computer systems.

MISSION COMMAND

2-76. Dedicated mission command personnel are needed in order to provide management and oversight of OSINT exploitation to ensure continued synchronization with maneuver elements, tasks, and requests.

ACQUISITION

2-77. Due to the volumes of publicly available information, acquisition through established information collection activities and systems are necessary in order to ensure that open-source information is not lost or misplaced that could provide essential and necessary mission-related information. Publicly available information acquired from open sources should be reported in accordance with established unit SOPs.

COLLECTING AND PROCESSING

2-78. OSINT properly integrated into overall collection plans during operations are used to satisfy CCIRs. In order to access the full array of domestic and foreign publicly available information, the processing of materials oftentimes requires OSINT support to personnel operating in the areas of document exploitation (DOCEX).

Note. Personnel engaging in the collecting and processing of information involving these aspects will require an understanding of those items and materials that are commonplace and those that could possess intelligence value. They must further be versed in the additional regulations for Director, National Security Agency (DIRNSA) oversight. Unless foreign publicly available information and open sources are collected and subsequently processed into a suitable form, the information will lose intelligence value.

PRODUCTION

2-79. Production of actionable and timely publicly available information through open sources is vital in OSINT exploitation. Research methods, Internet techniques (basic and advanced), and other associated tools are utilized to retrieve, integrate, evaluate, analyze, and interpret information into OSINT. Research information and finalized metadata as products are stored in databases accessible to other intelligence and nonintelligence personnel that have vested OSINT exploitation requirements.

COMPUTER SYSTEMS

2-80. OSINT personnel conducting OSINT exploitation need to have software allocated to the appropriate task. The necessary unfettered exploitation suite includes such programs as Analyst Notebook, Portable Document Format (PDF) Maker, and Text Chart.

Chapter 3

Collecting OSINT

Due to the unclassified nature of publicly available information, those engaging in OSINT collection activities can begin researching background information on their assigned area of responsibility long before the issuance of an official military deployment order while generating intelligence knowledge. IPB, an integrating process for Army forces, is the mechanism identifying intelligence and information requirements that can be satisfied utilizing publicly available information and open sources.

COLLECTING PUBLICLY AVAILABLE INFORMATION

3-1. Publicly available information and open-source research, applied as an economy of force, is an effective means of assimilating authoritative and detailed information on the mission variables (METT-TC) and operational variables (political, military, economic, social, information, infrastructure, physical environment, time [PMESII-PT]). The compilation of unanswered intelligence and information requirements determined at the conclusion of the MDMP and IPB are exercised through the commander's input. Commander's input—

- Is expressed in the terms of describe, visualize, and direct.
- Is the cornerstone of guidance used by OSINT personnel.
- Validates intelligence and information requirements.

3-2. Commander's input is expressed as CCIRs and categorized as friendly force information requirements (FFIRs) and PIRs. Continuous research and processing methods, coupled with the commander's input and intelligence and information requirements, OSINT personnel collect publicly available information for exploitation. The *collect* step of the intelligence process involves collecting, processing, and reporting information in response to information collection tasks. Collected information is the foundation of intelligence databases, intelligence production, and situational awareness.

3-3. OSINT is integrated into planning through the continuous process of IPB. Personnel engaging in OSINT exploitation must initiate collection and requests for information to satisfy CCIRs to the level of detail required. Collecting open-source information comprises four steps, as shown in figure 3-1 on page 3-2:

- Identify information and intelligence requirements.
- Categorize intelligence requirements by type.
- Identify source to collect the information.
- Determine collection technique.

IDENTIFY INFORMATION AND INTELLIGENCE REQUIREMENTS

3-4. Intelligence and information gaps are identified during the IPB process. These gaps should be developed and framed around the mission and operational variables in order to ensure the commander receives the information needed to support all lines of operations or lines of effort. As information and intelligence are received, OSINT personnel update IPB products and inform the commander of any relevant changes. OSINT needs clearly stated information and intelligence requirements to effectively focus

acquisition and production and should be incorporated into collection plans in order to satisfy these requirements.

Note. OSINT cannot eliminate all the unknown aspects or uncertainties that concern commanders and staffs. The G-2/S-2 must be prepared to fill gaps with reasonable assumptions; once gaps are filled, the G-2/S-2 must begin developing databases at the unit level in order to have information readily available. This reduces the number of new requests for information from subordinate units or organizations.

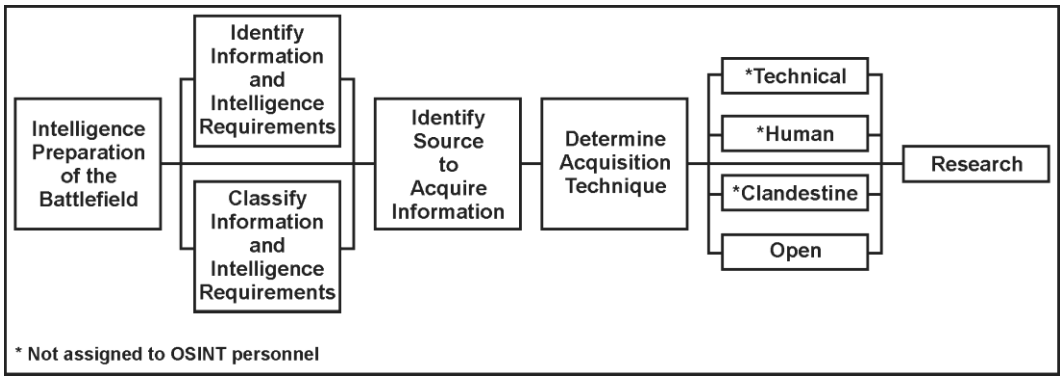


Figure 3-1. Process for collecting publicly available information

CATEGORIZE INTELLIGENCE REQUIREMENTS BY TYPE

3-5. Intelligence requirements that need to be satisfied can extend beyond the scope of OSINT, resulting in gaps. OSINT is subject to information and intelligence gaps that need to be satisfied using other appropriate methods to close those gaps.

3-6. IPB is used to classify intelligence and information requirements by type based on mission analysis and friendly COAs. OSINT personnel provide input during this step. Two important related terms that work in concert with OSINT are private information and publicly available information:

- **Private information** comprises data, facts, instructions, or other material intended for or restricted to a particular person, group, or organization. Intelligence requirements that require private information are not assigned to OSINT sections. There are two subcategories of private information:
 - ***Controlled unclassified information*** requires the application of controls and protective measures, for a variety of reasons (that is, *sensitive but unclassified* or *for official use only*).
 - ***Classified information*** requires protection against unauthorized disclosure and is marked to indicate its classified status when produced or disseminated.
- **Publicly available information** comprises data, facts, instructions, or other material published or broadcast for general public consumption; available on request to a member of the general public; lawfully seen or heard by any casual observer; or made available at a meeting open to the general public.

Note. The amount of classified information produced on any one topic can be limited and taken out of context if viewed from a solely classified perspective. OSINT validation is necessary when dealing with a large amount of classified information. OSINT validation is used when classified sources are unavailable or to confirm or support preexisting classified sources. This strengthens the credibility of OSINT products in support of all-source intelligence. OSINT validation provides the ability to cue other assets thus enhancing the accuracy and precision of gained intelligence.

IDENTIFY SOURCE TO COLLECT INFORMATION

3-7. Identifying the source is part of planning requirements and assessing collection plans. The two types of sources used to collect information are confidential sources and open sources:

- **Confidential sources** comprise any persons, groups, or systems that provide information with the expectation that the information, relationship, or both are protected against public disclosure. Information and intelligence requirements that require confidential sources are not assigned to OSINT sections.
- **Open sources** comprise any person or group that provides information without the expectation of copyright or privacy—the information, the relationship, or both is not protected against public disclosure. Open sources include but are not limited to—
 - ***Academia.*** Courseware, dissertations, lectures, presentations, research papers, and studies in both hardcopy and softcopy covering subjects and topics on economics, geography (physical, cultural, and political-military), international relations, regional security, and science and technology.
 - ***Government agencies and nongovernmental organizations.*** Databases, posted information, and printed reports on a wide variety of economic, environmental, geographic, humanitarian, security, and science and technology issues.
 - ***Commercial and public information services.*** Broadcasted, posted, and printed news on current international, regional, and local topics.
 - ***Libraries and research centers.*** Printed documents and digital databases on a range of topics.
 - ***Individuals and groups.*** Handwritten, painted, posted, printed, and broadcasted information on subjects and topics on art, graffiti, leaflets, posters, tattoos, and Web sites.
 - ***Gray literature.*** Materials and information that are found using advanced Internet search techniques on the Deep Web consisting of technical reports, scientific research papers, and white papers.

DETERMINE COLLECTION TECHNIQUE

3-8. Collection implies gathering, by a variety of means, raw data and information from which finalized intelligence is then created or synthesized, and disseminated. Collected information is analyzed and incorporated into all-source and other intelligence discipline products. These products are disseminated per unit SOPs, OPORDs, other established feedback mechanism, or intelligence architecture. These techniques confirm the presence of planned targets and provide a baseline of activity and information on sources within the AO for further development and future validation. When gathering information, the utilized technique includes specific information requests, objectives, priorities, timeframe of expected activity, latest (or earliest) time the information is of value (LTIOV), and reporting instructions.

3-9. Open-source information that satisfies a CCIR is disseminated as quickly as possible to the commander and other staff personnel per unit SOPs or OPORDs. OSINT can use unintrusive collection techniques to cue more technical collection assets. Collection techniques, depending on operation complexities, can enhance the chances of satisfying intelligence and information requirements.

3-10. Open-source acquisition of information and intelligence requirements are assigned to OSINT personnel. Open-source collection includes the acquisition of material in the public domain. The extent to which open-source collection yields valuable information varies greatly with the nature of the target and the subject involved. The information might be collected by individuals who buy books and journals, observe military parades, or record television and radio programs.

RESEARCH

3-11. After determining the collection technique, OSINT personnel conduct research to satisfy intelligence and information requirements.

3-12. Research—

- Leads to the population of information and intelligence databases. These databases enable OSINT personnel to accurately respond to changes within the AO by providing requested information to satisfy requirements.
- Is used to gather information that contributes to providing an understanding of a problem and organizing the results comprehensively.
- Is used to generate intelligence knowledge before and during deployments.

3-13. Two types of research methods that can be used are—

- **Field research.** Personnel from academic, governmental, intergovernmental, and nongovernmental organizations acquire data from primary sources, as well as retrieve data and information from secondary sources. Field research—
 - Consists of participant observation, data collection, and survey research.
 - Is typically conducted at the operational and strategic levels when time is not a factor in the development of information and intelligence of the operational variables (PMESII-PT) to provide commanders situational awareness.
- **Practical research.** Intelligence personnel retrieve existing data and information from secondary sources. Practical research—
 - Is typically conducted at the tactical level when time is a factor in the development of information and intelligence of the mission variables (METT-TC) in providing commanders situational awareness.
 - Is primarily used among intelligence personnel that engage in OSINT exploitation.

3-14. All research begins with the determination of a research question and the development of a research plan.

DETERMINE RESEARCH QUESTION

3-15. Research begins with the determination of a research question expressed in the form of CCIRs regarding a given topic. In OSINT exploitation, the research question can be based on the mission variables (METT-TC) and operational variables (PMESII-PT). The research question is refined through the development of information and intelligence requirements to be satisfied. Those requirements that are not satisfied are included in the planning requirements and assessing collection plan where more technical means of collection can be utilized.

DEVELOP RESEARCH PLAN

3-16. Different facets of a question may be expressed as information and intelligence requirements. These requirements form the basis for the research plan. A research plan can use both field research and practical research. The plan consists of—

- Identification of information sources (both primary and secondary).
- Description of how to access those sources.
- Format for compiling the data.
- Research methodology.
- Dissemination format.

IMPLEMENT RESEARCH PLAN

3-17. Utilizing open-source media—the means of sending, receiving, and recording information—components, and associated elements (see table 3-1), OSINT personnel implement a research plan. The primary media used to implement a research plan include—

- Public speaking forums.
- Public documents.
- Public broadcasts.
- Internet Web sites.

Note. The table does not illustrate an all-inclusive list of open-source media types but rather the categories of open-source media to consider when collecting open-source information.

Table 3-1. Open-source media, components, and elements

Media	*Components*	*Elements*	
Public Speaking	Speaker	• Sponsor • Relationship	• Message
	Format	• Conference • Debate • Demonstration • Speeches	• Lecture • Rally • Loud speakers • Talk shows
	Audience	• Location	• Composition
Public Documents	Graphic	• Drawing • Engraving • Painting • Graffiti	• Photograph • Print • Posters
	Recorded	• Compact data storage device • Digital video disk	• Hard disk • Tape
	Printed	• Book • Brochure • Newspapers • Magazines • Government releases • “Dumpster diving” • Annuals	• Periodical • Pamphlet • Report • Novelties • Non-government releases • Leaflets • Business cards
Public Broadcasts	Radio	• Low frequency AM radio • Medium frequency AM radio • Short wave radio	• VHF FM radio • Satellite radio • Standard wave radio
	Television	• Ku band satellite television • VHF and UHF terrestrial television • Advertisements • Motion pictures	
Internet Web Sites	Communications	• Chat • E-mail • News; newsgroup	• Web cam • Web cast • Web log
	Databases	• Commerce • Education	• Government • Military organizations
	Information (Web page content)	• Commerce • Education	• Government • Military organizations
	Services	• Dictionary • Directory • Downloads • Financial	• Geospatial • Search and URL lookup • Technical support • Translation

AM	amplitude modulation	URL	uniform resource locator
FM	frequency modulation	VHF	very high frequency
UHF	ultrahigh frequency		

Public Speaking Forums

3-18. OSINT personnel conduct research by attending public speaking forums such as conferences, lectures, public meetings, working groups, debates, and demonstrations. Attending these and similar events are opportunities to build relationships with nonmilitary professionals and organizations. Intelligence personnel require a thorough understanding of the local culture and laws to ensure any collection activities are unintrusive and do not violate local customs or laws, such as the Chatham House Rule. It is recommended to have the SJA's oversight during such collection missions to ensure compliance with AR 381-10, procedure 10. OSINT personnel require situational awareness and cultural understanding that is typically done by establishing both military and nonmilitary relationships with attendees, identifying any modifications of a speaker's message, and identifying personnel of interest attending the event.

3-19. OSINT personnel engaging in open-source exploitation, utilize public speaking forums typically in operational environments dominated by either stability operations or counterinsurgency operations where the level of violence is low.

Note. The Chatham House Rule states, "When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speakers, nor any other participants, may be revealed." Questioning the invocation of the Chatham House Rule should be inquired before the engagement begins. An invoked Chatham House Rule changes the characterization of the source from an open to a confidential source and may demand collection restrictions to ensure compliance with intelligence oversight limitations. (See appendix A.)

Public Documents

3-20. When acquiring public documents, OSINT personnel must be aware of the local environment and use a technique that is unintrusive and appropriate for the situation. These techniques include but are not limited to—

- Photographing and copying documents available in public forums such as town halls, libraries, and museums.
- Finding discarded documents in a public area such as streets, markets, and restrooms.
- Photographing documents in public areas such as banners, graffiti, and posters.
- Purchasing documents directly from street vendors, newspaper stands, book stores, and publishers.
- Purchasing documents through a third party such as a wholesale distributor or book club.
- Receiving documents upon request without charge from the author, conferences, trade fairs, direct mail advertising.

Public Broadcasts

3-21. Regional bureaus of the DNI OSC collect on regional and international broadcast networks in accordance with open-source information and intelligence requirements. Coverage of regional and international broadcasts enables OSINT personnel and organizations to use assets from already identified sources. The four techniques used to acquire information of public broadcasts are—

- **Spectrum search.** Searching the entire spectrum to detect, identify, and locate all emitters to confirm overall activity. This search provides an overview of the amount and types of activities and where they are located in the spectrum.
- **Band search.** Searching a particular segment of the spectrum to confirm overall activity. By limiting the size of the search band, the asset can improve the odds of acquiring a signal.
- **Frequency search.** Searching for radio or television frequencies.
- **Program search.** Searching for radio or television programs. Programs vary by type, content characteristics, and media format. Program surveillance verifies and expands upon initial results.

Note. For best results, OSINT personnel should use these techniques in combination rather than independently to generate intelligence knowledge. The selection of the techniques depends on the mission, the number of personnel, and capabilities.

3-22. For detailed information on collecting information from public broadcasts, see the DNI OSC.

Internet Web Sites

3-23. The four steps to acquire information on Internet Web sites are—

- Plan Internet search.
- Conduct Internet search.
- Refine Internet search.
- Record results.

3-24. For more detailed information on research using Internet Web sites, see appendix C.

Chapter 4

Producing OSINT

The Army operates in diverse environments around the world. This diversity requires proper use of publicly available information and open sources in the production of OSINT. Given the volume of existing publicly available information and the unpredictability of requests for information and intelligence requirements, OSINT personnel engaging in open-source exploitation must be fluidly aware of and flexible when producing OSINT. Effective production ensures that commanders and subordinates receive timely, relevant, and accurate intelligence. OSINT personnel produce OSINT by evaluating, analyzing, reporting, and disseminating intelligence as assessments, studies, and estimates.

CATEGORIES OF INTELLIGENCE PRODUCTS

4-1. After receiving a mission through the MDMP and commander's intent—expressed in terms of *describe*, *visualize*, and *direct*—intelligence and information requirements are identified. Personnel engaging in OSINT exploitation typically gather and receive information, perform research, and report and disseminate information in accordance with the categories of intelligence products. (See table 4-1.) OSINT products are categorized by intended use and purpose. Categories can overlap and some publicly available and open-source information can be used in more than one product. (For more detailed information on the categories of intelligence products, see FM 2-0.)

Table 4-1. Categories of intelligence products

Indications and Warning
Indications and warning are intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve an threat to the United States, U.S. ally, or U.S. citizens abroad. It includes forewarning of hostile actions or intentions against the United States, its activities, overseas forces, or allied/coalition nations (JP 2-0).
Current Intelligence
Current intelligence supports ongoing operations; it involves the integration of time-sensitive, all-source intelligence and information into concise, accurate, and objective reporting on the area of operations (AO) and current threat situation. One of the most important forms of current intelligence is the threat situation portion of the common operational picture. The intelligence officer is responsible for producing current intelligence for the unit. In addition to the current situation, current intelligence should provide projections of the threat's anticipated actions and their implications on the friendly operation. (See JP 2-0.)
General Military Intelligence
General military intelligence is intelligence concerning (1) military capabilities of foreign countries or organizations or (2) topics affecting potential U.S. or multinational military operations relating to armed forces capabilities, including threat characteristics, organization, training, tactics, doctrine, strategy, and other factors bearing on military strength and effectiveness and area terrain intelligence… (excludes scientific and technical intelligence (JP 2-0). This broad category of intelligence is normally associated with long-term planning at the national level. ***Note.*** This definition was shortened for brevity. The complete definition is available in JP 2-0.

Table 4-1. Categories of intelligence products (continued)

Target Intelligence
Intelligence that portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance (JP 3-60). Target intelligence is the analysis of threat units, dispositions, facilities, and systems to identify and nominate specific assets or vulnerabilities for attack, reattack, or exploitation. It consists of target development and combat assessment. Target development is the systematic evaluation and analysis of target systems, system components, and component elements to identify high-value targets for potential engagement through lethal or nonlethal means. Combat assessments provide a timely and accurate estimate of the effects of the application of military force (lethal or nonlethal) and mission command warfare on targets and target systems based on predetermined objectives.
Scientific and Technical Intelligence
Scientific and technical intelligence is the product resulting from the collection, evaluation, analysis, and interpretation of foreign scientific and technical information. Scientific and technical intelligence covers foreign developments in basic and applied research and in applied engineering techniques and scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel, the related research and development, and the production methods employed for their manufacture (JP 2-01).
Counterintelligence
Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities (EO 12333). Counterintelligence analyzes the threats posed by foreign intelligence and security services, and international terrorist organizations, and the intelligence activities of non-state actors such as organized crime, terrorist groups, and drug traffickers.
Estimative
Intelligence that identifies, describes, and forecasts adversary capabilities and the implications for planning and executing military operations (JP 2-0). Estimates provide forecasts on how a situation may develop and the implications of planning and executing military operations. Estimative intelligence goes beyond descriptions of threat capabilities or reporting of threat activity and tries to forecast the unknown based on an analysis of known facts using techniques such as pattern analysis, inference, and statistical probability.

EVALUATE INFORMATION

4-2. Open sources are overt and unclassified. Due to these aspects of publicly available information and open sources, deception, bias, and disinformation are of particular concern when evaluating sources of information during OSINT exploitation. Information is evaluated in terms of—

- Communications.
- Information reliability and credibility.

COMMUNICATIONS

4-3. A simple communications model is typically two-way and consists of six parts:

- Intended message.
- Speaker (sender).
- Speaker's encoded message.
- Listener (receiver).
- Listener's decoded message.
- Perceived message.

4-4. The speaker and listener each have different perspectives and aspects of communications (as shown in table 4-2 on page 4-4). There are great challenges facing communicators as the message becomes encoded by the speaker and decoded by the listener.

4-5. Communications during public speaking engagements are often difficult to evaluate given the myriad of elements that can prevent a successfully transmitted message. Given the multiple elements taken simultaneously, public speaking events are subjective and can be misunderstood.

4-6. The speaker has an intended message through a verbal, nonverbal, vocal, or visual media channel or combination thereof. Within communications, the areas typically involved in preventing the true intent of the message are the sending method, environment, and receiving method. Having an understanding of these areas generally yields a greater success rate between the speaker and listener.

4-7. Verbal communication begins with a speaker imparting or interchanging thoughts, opinions, or information. This communication can be either positive or negative. The typical speaker has a communication type:

- Passive.
- Aggressive.
- Passive-aggressive.
- Assertive.

4-8. Speakers communicate verbally and nonverbally based on their beliefs, emotions, or goals. These types of communication are indicated in table 4-2 on page 4-4. It is important to understand the differences in communication styles, how they are interpreted by an audience in order to effectively communicate the message intended and avoid misunderstandings. Evaluating information acquired through public speaking venues can be challenging based on these factors. Using the table to compare these types of communication can assist collection personnel in determining the influences surrounding communicators and predicting how the messages may be perceived. Table 4-2 illustrates and provides a guideline to assist in determining the type of displayed behavior, beliefs, emotions, and goals.

Note. Table 4-2 is not intended to stand alone but used in support of all-source intelligence. Publicly available information and open sources are used to develop personality and characteristic traits of an individual. These traits include previous speeches, lectures, sermons, or statements that are used to determine a baseline of anticipated behavior and responses. There are external influences that can positively or negatively affect an individual. These external influences include but are not limited to consequences of disputing a superior's opinion, the atmosphere or setting (such as academic, religious, or political), or an impromptu public interview using a question and answer format.

INFORMATION RELIABILITY AND CREDIBILITY

4-9. OSINT personnel evaluate information with respect to reliability and credibility. It is important to evaluate the reliability of open sources in order to distinguish objective, factual information; bias; or deception. The rating is based on the subjective judgment of the evaluator and the accuracy of previous information produced by the same source.

4-10. OSINT personnel must assess the reliability and the credibility of the information independently of each other to avoid bias. The three types of sources used to evaluate and analyze received information are—

- **Primary sources.** Have direct access to the information and conveys the information directly and completely.
- **Secondary sources.** Conveys information through intermediary sources using the vernacular and summarizes or paraphrases information.
- **Authoritative sources.** Accurately reports information from the leader, government, or ruling party.

Note. Secondary and authoritative sources, such as government press offices, commercial news organizations, political campaign staffs, research center publications, newspapers, periodicals, databases, and libraries, can intentionally or unintentionally add, delete, modify, or filter the information made available to the public.

Table 4-2. Comparison of communication types

	Passive	*Aggressive*	*Passive-Aggressive*	*Assertive*
Behavior	• Keeps quiet. • Does not say what is actually felt, needed, or wanted. • Frequently puts oneself down. • Apologizes when expressing oneself. • Denies feelings of disagreements or indifferences.	• Expresses feelings and wants as though any other view is unreasonable or stupid. • Dismisses, ignores, or insults the needs, wants, and opinions of others.	• Fails to meet the expectations of others through 'deniable' means (such as forgetting or delays). • Denies personal responsibility for actions.	• Expresses needs, wants, and feelings directly and honestly. • Does not assume correctness or everyone feels similar. • Allows others to hold other views without dismissal or insults.
Nonverbal Communication	• Minimizes oneself. • Looks down, hunches shoulders, avoids eye contact. • Speaks softly.	• Enlarges oneself and appears threatening. • Eye contact is fixed and penetrating. • Voice is loud, perhaps shouting.	• Typically mimics the passive style.	• Body is relaxed, and movements are casual. • Eye contact is frequent but not glaring.
Beliefs	• Others' needs are more important. • Others have more rights. • Others' contributions are more valuable.	• Personal needs are more important and more justified than others'. • Others have no personal rights. • Personal contributions are more valuable.	• Entitled to get own way, even after making commitments to others. • Not responsible for personal actions.	• Everyone's needs are equally important. • Everyone has equal rights to be expressive. • Everyone has valuable contributions. • Responsible for personal behavior.
Emotions	• Fears rejection. • Feels helpless, frustration, and anger. • Bears resentment toward others' mistreatment. • Has reduced self-respect.	• Angry or powerful at the time of victory. • Feels remorse, guilt, or self-hatred for hurting others.	• Fears assertiveness. • Resents the demands of others. • Fears of being confronted.	• Feels positive about oneself and the treatment of others. • High level of self-esteem.
Goals	• Avoids conflict. • Pleases others at any expense. • Gives others control.	• Wins at any expense to others. • Gets control over others.	• Gets personal way without having to take responsibility.	• Self-respect is kept by everyone. • Expresses oneself without having to win all the time. • No one controls anyone else.

4-11. Nonauthoritative sources lack reliability and trustworthiness and seldom stand apart from authoritative sources. The information provided by nonauthoritative sources generally does not support topics agreed upon as being true and reliable in academia. Nonauthoritative sources also make finding additional in-depth information difficult to locate.

4-12. Nonauthoritative sources are generally unavailable and inaccessible by the public. Nonauthoritative sources are uncorroborated by multiple public sources of information. Examples of nonauthoritative sources include but is not limited to—

- Unreviewed documents from self-published Web repositories such as blogs, Wikipedia, political sites, and commercial advertising.
- Material received via uncorroborated e-mail, hearsay, or statements solely in oral form.
- Informal personal communications such as letters to the editor and opinion essays.

4-13. When evaluating sources of information to determine reliability and credibility consider—

- **Identity.** *Who* produced the information (for example a student, teacher, political organization, or reporter)?
- **Authority.** *How* much does the source know about the information?
- **Motive.** *Why* was the information published?
- **Access.** Did the source have direct access to the event or information?
- **Timeliness.** *What* is the date of the information?
- **Internal and external consistency.** Does the information contradict governmental policies among local citizens?

PROCESS INFORMATION

4-14. *Process* is an information management activity: to raise the meaning of information from data to knowledge (FM 6-0). The function of processing, although not a component of the intelligence process, is a critical element in the analyzing and producing of OSINT. Publicly available information answers intelligence and information requirements. Based on the type of information received, it must be processed before being reported and disseminated as finalized OSINT. Intelligence personnel transform publicly available information and open sources into a form suitable for processing by—

- Digitizing.
- Transcribing and translating.

DIGITIZING

4-15. OSINT personnel create a digital record of documents by scanning or taking digital photographs. Pertinent information about the document must be annotated to ensure accountability and traceability. Digitization enables the dissemination of the document to external databases and organizations, as well as enables the use of machine translation tools to screen documents for keywords, names, and phrases.

TRANSCRIBING AND TRANSLATING

4-16. A *transcript* refers to a written verbatim, native language rendering of the spoken words in an audio or video recording. Both listening and writing proficiency in the source language are essential for an accurate transcript. The transcript includes descriptions of the activity, background, and conditions that the transcriber hears in the audio and observes in the video. The linguist uses online dictionaries, gazetteers, working aids, and software to improve the transcript. Once completed, the transcription is sent to a quality control linguist.

4-17. A *translation* is not verbatim but an approximation of the literal and implied meaning of the foreign language. The linguist must be able to read and comprehend the source language, write comprehensibly in English, and choose the equivalent expression in English that fully conveys and best matches the meaning intended in the source language.

4-18. During processing, a linguist creates either an extract, a summary, or a full translation of the original document or transcript into a standardized format established by unit SOPs. The linguist uses online dictionaries, gazetteers, working aids, and software to improve the translation. Once completed, the translation is sent to a quality control linguist.

4-19. Linguists perform quality control reviews of each transcription and translation to ensure both quality and consistency with established unit SOPs. A U.S. Government or military linguist should review all information that a non-U.S. Government linguist processes with exceptions involving long-term multinational partners of the United States and U.S. contractors with the requisite skills and the confidence of the command. Linguistic quality control is an important facet to process foreign publicly available information. Each transcription and translation undergoes two levels of review:

- **Quality control.** During quality control, a qualified linguist ensures that the transcription or translation is accurate, complete, free of bias, and in accordance with reporting and dissemination standards. The U.S. linguist returns the transcript or translation for correction, adds or corrects missed content, or corrects minor format errors. Upon completion of quality control, the transcription or translation is available for processing.
- **Quality assurance.** During quality assurance, a qualified U.S. linguist or OSINT analyst reviews the transcript or translation to ensure that it contains all required information and reads naturally in English. Once reviewed, the completed transcription or translation is saved to internal databases to be processed for reporting and dissemination.

ANALYSIS OF MEDIA SOURCES

4-20. Analysis of the media is the systematic comparison of the content, behavior, patterns, and trends of organic media organizations and sources of a country. Analysis of the media as an activity was developed and based on methods and experience gained during OSINT exploitation against authoritarian political systems during the World War II and Cold War eras where media was government-controlled. Publicly available information and open sources must be analyzed for proper inclusion in OSINT processing. OSINT personnel weigh media analysis against set criterion. These criterions assist OSINT personnel to discern facts, indicators, patterns, and trends in information and relationships. This involves inductive or deductive reasoning to understand the meaning of past events and predict future actions.

4-21. Comparison of trends in the content of individual media with shifts in official policy suggests that some media continues to mirror the dominant policy line. By establishing a track record for media that is vulnerable to external and internal pressure to follow the central policy line, OSINT personnel can identify potential policy shifts. Comparison of *what is said* and *what is not said* against the background of *what others are saying* and *what has been said before* is the core of media source analysis.

4-22. Media source analysis is also important in semi-controlled and independent media environments. In media environments where both official and nonofficial media are present, official media may be pressured to follow the central policy line. Analyzing media in these environments must encompass both the journalist and commentator level. It is important to establish the track record of such individuals to discover access to insider information from parts of the government or being used by officials to float policies.

Note. Differences in content between media outlets controlled by different official elites can reveal policy and leadership disputes. For example, a report on a speech by the President covered by government-controlled media may reveal differences from reports covering the same speech in either a semi-controlled or independent media environment.

4-23. The three aspects of media source analysis are—

- Media control.
- Media structure.
- Media content.

Media Control

4-24. Analyzing media environments in terms of media control requires awareness by intelligence personnel of how different elements of the media act, influence, and are of intelligence value. Careful examination of the differences in how media is handled in different types of environments can provide insight into domestic and foreign government strategies. Media environments are categorized as—

- **Government-controlled.**
 - Control over the media is centralized.
 - The dominant element of control is the government and higher tiers of political leadership.
 - Governments use censorship mechanisms to exercise control over media content prior to dissemination of information.
- **Semi-controlled.**
 - Control over the media is semi-centralized.
 - Governments exercise and promote self-censorship by pressuring media managers and journalists prior to dissemination of information.
- **Independent.**
 - Control over the media is decentralized.
 - Governments may regulate allocation of broadcast frequencies, morality in content, ownership in media markets, and occasionally apply political pressure against media or journalists.
 - Economic factors, norms of the journalist profession, the preferences of people who manage media, and the qualities of individual journalists who report or comment on the news all influence or control media content.

4-25. All media environments are controlled to some degree and therefore easier to perform media source analysis. The challenge for OSINT personnel is to determine the level, factors, and elements (see table 4-3) that elites, institutions, or individuals exercise control, how much power each possesses, and what areas are of interest to satisfy intelligence and information requirements.

Table 4-3. Level, factors, and elements of media control

Level	*Factor*	*Elements*
Political	The laws and norms governing operations of the media, officials, and the distribution of power	• Top leadership consensus • Top leaders individually • Institutions
Journalist	The degree of freedom afforded to the media by the political system that is subordinated from media executives, to media managers, and to individual journalists	• Board of directors of media companies • Individual directors • Influential shareholders • Managing editors • Department editors • Program producers • Anchors • Individual journalist
Individual	The laws and norms governing the appearance and behavior of individuals in the media	• Group of subjects or participants • Individual subject or participant

Media Structure

4-26. Media structure encompasses attributes of media material. There are structural elements that affect the meaning and significance of the content of the item and are often as important as the content itself. Analysis of these elements uncovers insights into the points of view of personnel in government-controlled, semi-controlled, and independent environments to establish the structure of media elements.

4-27. The media structural elements are—

- Selection, omission, and slant.
- Hierarchy of power.
- Format.
- Media type.
- Prominence.
- Dissemination.
- Timing.

Selection, Omission, and Slant

4-28. Selection of media items is a fundamental editorial decision at the core of news reporting. Selection includes media manager decisions about which stories are covered, which stories are not covered, and which slant (viewpoint), images, and information should be included, emphasized, deemphasized, or omitted in a news item.

Hierarchy of Power

4-29. All political systems involve a hierarchy of power (see table 4-4) that logically follows official statements issued by elements in corresponding hierarchy of authoritativeness. Authoritativeness is the likelihood that the views expressed in the statement represent the dominant viewpoint within the political system. The hierarchy is obvious at the political level—a statement by the prime minister trumps a statement by a minister. In other cases, the hierarchy may not be so obvious—a speech by the party chairman is more authoritative than the head of state.

Table 4-4. Hierarchy of media power

Information Type	*Purpose*	*Example*
Reports	Inform the viewer, listener, or reader	Authoritative or nonauthoritative based on track record
Commentary and editorials	State a position or opinion and persuade the viewer, listener, or reader	**Commentators** Authoritative: • Know pseudonym of top leader • Known advisor to Prime Minister • Associated with major party • Contributor to a major paper **Editors** Authoritative: • Ruling party's leaders or large donors • Large segment of political or financial elite • Large numbers of voters or small campaign contributors • Small segment of voters or population with special interests or radical views • Local officials and citizens
Official Statement	Declaration of policy or position by an officer or an executive body of the government or ruling party	Authoritative: • President • Secretary of State • State Department spokesperson

Format

4-30. Format consists of how media is produced and disseminated for public consumption. Format can be in the form of a live news report, a live interview, or a prerecorded report or interview that gives individuals more opportunity to influence the context delivered to consumers.

Media Type

4-31. Television is the medium with the largest potential audience in media environments and has a significant impact in shaping the impressions of the general viewing public. Television has replaced radio as the main source of news except in media environments where poverty prevents mass access to television. Fewer people may get information from newspapers and Internet news Web sites, but these people may be richer, better educated, and more influential than the general television audience. Specialized print publications and Internet Web sites reach a still smaller audience, but the audience will likely include officials and experts who that have influence on policy debates and outcomes.

Prominence

4-32. Questions to consider pertaining to prominence of media stories are—

- Does the story appear on the front page of newspapers or on the homepage of news Web sites?
- How much space is the story given?
- In what order does the story appear in the news broadcast?
- Is it featured in the opening previews of the newscast?
- How frequently is the story rebroadcast on subsequent newscasts or bulletins?
- How much airtime did it get?

Dissemination

4-33. Attention to patterns of dissemination of leader statements is important in government-controlled media environments. Leaders communicate publicly in a variety of ways such as formal policy statements, formal interviews, and impromptu remarks. By comparing the volume of media attention given to a statement, determination is made to whether the statement was intended to be taken as a pronouncement of established policy or merely as an ad hoc, uncoordinated expression prompted by narrow contextual or temporal conditions.

Timing

4-34. OSINT personnel have traditionally paid close attention to the timing of the appearance of information in the media as the information corresponds to the news cycle. A news cycle is the process and timing by which different types of media sources obtain information, incorporate or turn the information into a product, and make the product available to the public.

Media Content

4-35. Understanding the significance of media content can enhance the value of media source analysis. Media content encompasses the elements of—

- Manifest content.
- Latent content.

Manifest Content

4-36. Manifest content is the actual words, images, and sounds conveyed by open sources. One of the most important forms of media source analysis involves the careful comparison of the content of authoritative official statements to identify the policies or intentions represented. Governments, political entities, and actors use statements and information released to the media to strengthen, support, and promote policies.

4-37. Manifest content analysis of authoritative public statements is an effective tool to discern leadership intentions and attitudes. Manifest content, in order to be effective, consists of the following:

- **Esoteric communications** or "reading between the lines" are public statements whose surface meaning (manifest content) does not reveal the real purpose, meaning, or significance (latent content) of the author. Esoteric communication is particularly evident in political systems with strong taboos against public contention or in cases where sensitive issues are at stake. Esoteric communication is more formalized in some media environments than in others but is common in all political communications.
- **Multimedia content** analysis considers elements of content beyond the words used such as facial expressions, voice inflections of leaders giving a speeches or while being interviewed, or the reading of a script by a news broadcaster all provide indicators about the views of a subject or topic. These indicators assist to determine whether a statement was seriously considered, intended to be humorous, or simply impromptu.
- **Historical or past behavior** of open sources must be considered. Influences such as media outlet, journalist, newsmaker, or news broadcaster are factors beyond immediate control. Other issues such as time pressures, deadlines, or technical malfunctions, may also affect the content or context of public information. Analysts' judgments about source behavior must be made with careful consideration of previous behavior.

Latent Content

4-38. Latent content refers to the hidden meaning of a thought. Latent content can reveal patterns about the views and actions of the media controllers. These patterns and rules come from the unstated content that provides the underlying meaning of media content and behavior. When a pattern of content is changed, inference of a change in the viewpoint of the controller or a change in the balance of power among different controlling elements has occurred.

REPORT AND DISSEMINATE INFORMATION

4-39. Intelligence and information requirements satisfied through publicly available information and open sources should be immediately reported and disseminated in accordance with unit SOPs that are generally centered on intelligence requirements, information criticality, and information sensitivity.

Note. Staff personnel not directly assigned to the OSINT section also acquire information that is incorporated within the running estimate of each staff element. Close cooperation between these individuals fosters a supportive environment about *what* and *how* to report information of potential operational or intelligence value through the proper channels.

4-40. Finalized OSINT serves no purpose unless it is timely, accurate, and properly disseminated to commanders and customers in a useable form. Reporting and disseminating a finalized OSINT product that satisfies intelligence and information requirements include but are not limited to—

- Single discipline or multidiscipline estimates or assessments.
- Statements of facts.
- Evaluations of threat capabilities and limitations.
- The threat's likely COAs.

REPORTING GUIDELINES AND METHODS

4-41. Effective dissemination creates a mechanism of feedback in order to assess usefulness and predict or assess future intelligence and information requirements. The objective in reporting and disseminating intelligence and information is to provide relevancy to support conducting (planning, preparing, executing, and assessing) operations.

4-42. The basic guidelines in preparing products for reporting and disseminating information are—

- **Timely.** Information should be reported to affected units without delay for the sole purpose of ensuring the correct format.
- **Relevant.** Information must contribute to the answering of intelligence requirements. Relevant information reduces collection, organization, and transmission times.
- **Complete.** Prescribed formats and SOPs ensure completeness of transmitted information.

4-43. The three reporting methods used to convey intelligence and information are—

- **Written.** Methods include formats (spot reports), tactical reports (TACREPs), or information intelligence reports (IIRs).
- **Graphic.** Web-based report dissemination is an effective technique to ensure the widest awareness of written and graphical information across echelons. OSINT personnel can collaborate and provide statuses of intelligence requirements through Web sites. Information can also be uploaded to various databases to support future open-source missions and operations.
- **Verbal and voice.** The most common way to disseminate intelligence and information verbally is through a military briefing. Based on the criticality, sensitivity, and timeliness of the information, ad hoc and impromptu verbal communication methods are the most efficient to deliver information to commanders.

SECURITY DOMAINS

4-44. OSINT is disseminated via security domains. A security domain is an application or collection of applications that share the same authentication or authorization. A security domain determines the overall classification of an enclave of servers, computers, or networks. Networks are separated by classification in order to prevent the compromise of information. OSINT organizations can exchange publicly available information on unclassified and classified networks across echelons between Army and other armed forces as well as joint organizations and federal, state, and local government agencies.

4-45. The replication of Web sites and databases from unclassified networks to classified networks ensure publicly available information, open sources, and finalized OSINT products are reported and disseminated to intelligence and nonintelligence personnel to support unified land operations. The establishment of an effective OSINT architecture involves the proper utilization of the three primary security domains:

- Joint Worldwide Intelligence Communications System (JWICS).
- SIPRNET.
- NIPRNET.

Joint Worldwide Intelligence Communications System

4-46. JWICS is a system of interconnected computer networks used by various U.S. Government departments to transmit TS/SCI over the transmission control protocol/Internet protocol (TCP/IP) suite in a secure environment. JWICS supports the synchronization of OSINT exploitation, dissemination of OSINT and supporting metadata, and collaboration between deployed and supporting intelligence personnel.

SECRET Internet Protocol Router Network

4-47. SIPRNET is a system of interconnected computer networks used by various U.S. Government departments to transmit classified information over the TCP/IP in a secure environment. SIPRNET is the principal mission-command data network at the tactical level. The network allows access to OSINT services and products through various databases, as well as gives intelligence and nonintelligence personnel the ability to collaborate, view, submit, and track OSINT intelligence and information requirements.

Nonsecure Internet Protocol Router Network

4-48. NIPRNET is used by various U.S. Government departments to exchange information up to the sensitive but unclassified level. NIPRNET is configured to provide access to Internet-based capabilities across all DOD components. It is the domain most commonly used to conduct open-source research and produce OSINT.

REPORTING AND DISSEMINATION CONSIDERATIONS

4-49. When reporting and disseminating OSINT products, considerations include but are not limited to—

- **Classification.** When creating products from raw information, write-to-release at the lowest classification level to facilitate the widest distribution of the intelligence. Use tearline report formats to facilitate the separation of classified and unclassified information for users operating on communications networks of differing security levels. Organizations with original classification authority or personnel with derivative classification responsibilities must provide subordinate organizations and personnel with a security classification guide or guidance for information and intelligence derived from publicly available information and open sources in accordance with the policy and procedures in AR 380-5.
- **Feedback-mechanism development.** E-mail, postal addresses, rating systems, and survey forms are mechanisms that OSINT personnel can use in order to understand the information requirements for customers.
- **Intellectual property identification.** Identify intellectual property that an author or an organization has copyrighted, patented, or trademarked taken to preserve rights to the information. OSINT exploitation does not involve the selling, importing, or exporting of intellectual property. OSINT personnel engaging in exploitation should cite all sources used in reported and disseminated products. When uncertain, OSINT personnel should contact the supporting SJA office before reporting and disseminating a finalized OSINT product.
- **Use of existing dissemination methods, when and if possible.** Creating new dissemination methods can at times complicate existing dissemination methods.
- **Analytical pitfalls.** Analysts need to be cognizant that there are pitfalls when reporting and disseminating OSINT. The errors, referred to as fallacies (omission and assumption), are usually committed accidentally although sometimes they are deliberately used to persuade, convince, or deceive. Analysts must also be aware of hasty generalization, false cause, misuse of analogies and languages, biases (cultural, personal, organizational, cognitive), and hindsight. (For more information on analytical pitfalls, see TC 2-33.4.)

Appendix A

Legal Restrictions and Regulatory Limitations

Publicly available information and open sources cover a wide array of areas. Exploring, assessing, and collecting publicly available information and open sources has the potential to adversely affect organizations that execute OSINT missions. In some regards, OSINT missions could involve information either gathered against or delivered by U.S. persons. Given the scope of OSINT and its applicability within the intelligence community, having a firm awareness of intelligence oversight and its regulatory applications is necessary.

EXECUTIVE ORDER 12333

A-1. All OSINT exploitation conducted by intelligence and nonintelligence personnel must comply with the legal restrictions, policies, and guidelines outlined in EO 12333 and other associated regulations, instructions, or directives.

A-2. EO 12333 states the goal of the national intelligence effort is to provide the President and the National Security Council the necessary information on which to base decisions concerning the conduct and development of foreign defense, economic policy, and protection of U.S. national interests.

A-3. EO 12333 originated from operations that DOD intelligence units conducted against U.S. persons involved in the Civil Rights and anti-Vietnam War movements. DOD intelligence personnel used overt and covert means to collect information on the political positions of U.S. persons, retained the information in a nationwide database, and disseminated the information to law enforcement authorities.

A-4. The purpose of EO 12333 is to enhance human and technical collection techniques, the acquisition of foreign intelligence, and the countering of international terrorist activities conducted by foreign powers especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities and espionage conducted by foreign powers. Accurate and timely information about the capabilities, intentions, and activities of foreign powers, organizations, and subordinate agents is essential to informed national defense decisions. Collection of such information is a priority objective, pursued in a vigorous, innovative, and responsible manner that is consistent with the U.S. Constitution and applicable laws and principles.

INTERPRETATION AND IMPLEMENTATION

A-5. AR 381-10 interprets and implements EO 12333 and DOD 5240.1-R. AR 381-10 enables the intelligence community to perform authorized intelligence functions in a manner that protects the constitutional rights of U.S. persons. The regulation does not authorize intelligence activity. An Army intelligence unit or organization must have the mission to conduct any intelligence activity directed against U.S. persons. In accordance with the Posse Comitatus Act (Section 1385, Title 18, USC), the regulation does not apply to Army intelligence units or organizations when engaged in civil disturbance or law enforcement activities without prior approval by the Secretary of Defense.

ASSIGNED FUNCTIONS

A-6. Based on EO 12333, the assigned intelligence functions of the Army are to—

- Collect, produce, and disseminate military-related foreign intelligence as required for execution of responsibility of the Secretary of Defense.
- Conduct programs and missions necessary to fulfill departmental foreign intelligence requirements.
- Conduct activities in support of DOD components outside the United States in coordination with the Central Intelligence Agency (CIA) and within the United States in coordination with the Federal Bureau of investigation (FBI) pursuant to procedures agreed upon by the Secretary of Defense and the Attorney General.
- Protect the security of DOD installations to include its activities, property, information, and employed U.S. persons by appropriate means.
- Cooperate with appropriate law enforcement agencies to protect employed U.S. persons, information, property, and facilities of any agency within the intelligence community.
- Participate with law enforcement agencies to investigate or prevent clandestine intelligence activities by foreign powers or international terrorists.
- Provide specialized equipment, technical knowledge, or assistance to U.S. persons for use by any department or agency, or, when lives are endangered, to support local law enforcement agencies.

ARMY REGULATION 381-10

A-7. AR 381-10 enables any Army component to perform intelligence functions in a manner that protects the constitutional rights of U.S. persons. It also provides guidance on collection techniques used to obtain information for foreign intelligence and CI purposes. Intelligence activity is not authorized by this regulation.

COLLECTION OF U.S. PERSON INFORMATION

A-8. Collection, in this context, is the gathering or receiving information by intelligence personnel in the course of official duties with the intent to use or retain the information for intelligence purposes. Action must be taken to demonstrate intended use of the collected information such as producing an intelligence information report, incident report, or adding the information to an intelligence database.

A-9. There must be a link between the collection of the U.S. person information and the intelligence agency assigned mission. This link is particularly important when dealing with publicly available information, open-source information, and information data exploitation.

A-10. Army intelligence components may collect U.S. person information by lawful means but must be limited to the least intrusive means feasible and shall not violate the law (see DOD 5240.1-R). These least intrusive collection means must be attempted before utilizing more intrusive collection means such as—

- Acquisition from publicly available sources or with the consent of the U.S. person of interest.
- If proven unfeasible or inefficient, acquisition from cooperating sources.
- If proven unfeasible or inefficient, acquisition from other lawful means that do not require a warrant or Attorney General approval.
- If proven unfeasible or inefficient, an approval request for the use of techniques requiring a warrant or Attorney General approval.

A-11. Within the United States, Army intelligence components may collect foreign intelligence concerning U.S. persons by overt means when the following conditions are met:

- The foreign intelligence sought is significant and does not concern the domestic activity of the U.S. person.
- The foreign intelligence cannot be reasonably obtained by overt means.

- Collection has been coordinated with the FBI in order to prevent the disruption of current operations.

A-12. The following considerations apply to the collection of U.S. person information from the Internet:

- Army intelligence components must use government computers to access the Internet for official government business unless otherwise authorized.
- IP addresses, uniform resource locators (URLs), and e-mail addresses that are not associated with a U.S. person may be acquired, retained, and processed by Army intelligence components without making an effort to determine association with a U.S. person as long as the component does not engage in analysis focused upon specific addresses.

A-13. AR 381-10 does not authorize the collection of any information relating to a U.S. person solely because of personal lawful advocacy of measures opposed to government policy as embodied in the First Amendment to the U.S. Constitution. The First Amendment states that Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

RETENTION OF U.S. PERSON INFORMATION

A-14. *Retention* refers only to maintaining information about U.S. persons that the Army intelligence component can retrieve by the person's name or other personal identifying data. AR 381-10, procedure 3, describes the kinds of U.S. person information that an Army intelligence component may knowingly retain without the individual's consent.

A-15. AR 381-10 authorizes the retention of U.S. person information under the following criteria:

- Information properly collected in accordance with AR 381-10, procedure 2.
- Army intelligence components acquired the information incidental to an otherwise authorized collection activity, and retained the information if it—
 - Could have been collected intentionally under the provisions of AR 381-10, procedure 2.
 - Is necessary to understand or assess foreign intelligence or CI.
 - Is foreign intelligence or CI collected from authorized electronic surveillance.

Note. *Electronic surveillance* refers to the acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

 - Is incidental to authorized collection and may indicate involvement in activities that may violate federal, state, local, or foreign law.
- Information relating to functions of other Army activities, DOD components, or non-DOD agencies. The information pertains solely to the functions and responsibilities of other activities, components or agencies, and is retained only as necessary to transmit the information to that agency. The transmittal is filed and destroyed under general correspondence records management. Army intelligence components will not retain the information in intelligence databases or repositories.

A-16. *Temporary retention* refers to the authorization for Army intelligence components to retain information up to 90 days, solely to determine if the information is, in fact, retainable under this regulation. The 90-day period starts upon receipt of the information.

A-17. *Other information* retained by Army intelligence components must be reported for oversight purposes and for necessary subsequent proceedings.

A-18. Access to U.S. person information retained in intelligence files, databases, and repositories is limited to those with a need to know the information. U.S. person information in intelligence files, databases, and

repositories is retained in accordance with disposition criteria in AR 25-400-2. Intelligence components will review intelligence files and databases annually. Intelligence components will specifically review U.S. person information to ensure its retention is still necessary to an assigned function. This ensures U.S. person information is not held beyond established disposition criteria, is retained for an authorized function, and was not retained in violation of this regulation. This does not apply to the Investigative Records Repository or other authorized long-term records holding areas.

DISSEMINATION OF U.S. PERSON INFORMATION

A-19. *Disseminate*, an information management activity, refers to communicating relevant information of any kind from one person or place to another in a usable form by any means to improve understanding or to initiate or govern action (FM 6-0). In other words, dissemination is the delivery of intelligence to users in a suitable form with application of the intelligence to appropriate missions, tasks, and functions. AR 381-10, procedure 4, governs the types of information regarding U.S. persons that Army intelligence organizations may disseminate without the person's consent outside the component which collected and retained the information.

QUESTIONABLE INTELLIGENCE ACTIVITY

A-20. Questionable intelligence activity occurs when intelligence operations potentially violate—

- Laws.
- EOs.
- Presidential directives.
- DOD or Army policies.

A-21. Intelligence personnel should report questionable intelligence activity through the chain of command, the inspector general, or directly to the Assistant to the Secretary of Defense for Intelligence Oversight in accordance with AR 381-10. The following are examples of questionable intelligence activity on improper collecting, retaining, or disseminating of U.S. person information:

- Collecting and gathering information about U.S. domestic groups not connected with a foreign power or international terrorism.
- Producing and disseminating intelligence threat assessments containing U.S. person information without a clear explanation of the intelligence purpose for which the information was collected.
- Collecting and gathering U.S. person information for force protection purposes without determining if the intelligence function is authorized.
- Collecting and gathering U.S. person information from open sources without a logical connection to the mission of the unit.

A-22. AR 381-10 directs intelligence organizations to refer questions concerning the interpretation of the instructions on collection, retention, and dissemination of U.S. person information to the local SJA's office.

ASSISTANT DEPUTY DIRECTOR OF NATIONAL INTELLIGENCE FOR OPEN SOURCE

A-23. The responsibilities of the ADDNI/OS include—

- Exercising the integration, evaluation, and oversight for the NOSE.
- Providing strategic oversight of and guides strategic involvement of OSINT.
- Chairing the National Open Source Committee (NOSC) and Open Source Board of Advisors.
- Overseeing the DNI OSC and the distributed NOSE.
- Ensuring the integration of the open-source collection management strategy.
- Developing oversight of the NOSE.
- Overseeing interagency sharing of open-source information.

INTELLIGENCE COMMUNITY

A-24. The responsibilities of the intelligence community include—

- Developing programmatic oversight and evaluation to be centralized under the ADDNI/OS.
- Supporting all intelligence disciplines.
- Establishing appropriate source and information validation and verification procedures of all open-source exploitation efforts.
- Developing metrics for overall open-source activities.
- Making all open-source information, products, and services available throughout the intelligence community.

NATIONAL OPEN-SOURCE COMMITTEE

A-25. The NOSC provides guidance to the NOSE. The responsibilities of the NOSC include—

- Developing appropriate operational standards for source or information verification, tradecraft, and training.
- Developing science and technology standards for metadata tagging and storage.

DIRECTOR OF NATIONAL INTELLIGENCE OPEN-SOURCE CENTER

A-26. The DNI OSC serves to advance the exploitation of open-source information through acquisition, procurement, analysis, and dissemination of products and services. The responsibilities of the DNI OSC include—

- Facilitating open-source exploitation for U.S. Government partners and customers.
- Securing appropriate licensing agreements for open-source customers.
- Developing open-source programs.
- Training personnel to properly exploit open-source information in accordance with security practices.

Appendix B

Cyberspace Internet Awareness

Intelligence and nonintelligence personnel conducting open-source research must be aware of the digital operational environment by minimizing and reducing cyber "footprints," practicing effective cyber OPSEC, utilizing safe online surfing techniques and habits, and understanding that embedded metadata can be contained in documents.

CYBERSPACE SITUATIONAL AWARENESS AND CYBER SECURITY

B-1. More than any other intelligence discipline, research involving publicly available information and open sources could unintentionally reveal CCIRs. Open-source research sometimes requires access to Internet Web sites that block browsing sessions originating from *.mil* or *.gov* sources. In the areas of computer information assurance and Internet security, internet awareness is needed in order to be effective, aggressive, and to successfully conduct open-source research and exploitation. Unjustified Internet Web-site restrictions have the potential to severely impede acquiring and the subsequent processing, reporting, and disseminating of publicly available information and open sources.

B-2. Awareness is the beginning of effective cyber security. Computers transmit machine specifications such as operating system, type of version of each enabled program, security levels, a history of Web sites visited, cookie information, user preferences, IP addresses, enabled languages, and referring URL when searching the Internet. Visitors are frequently redirected to alternate Web sites based on search criterion, location, language, and time the search is conducted.

B-3. The Internet is described as a "network of networks" due to the hundreds of thousands of interconnected networks consisting of millions of computers. Computers and users connected to the Internet are identified by a system-specific IP address that designates location. The IP address serves as the address where transferred information and datum is delivered. The concern therein rests in the understanding that while visiting nonstandard or questionable Internet Web sites in accordance with official duties, sensitive unit information could inadvertently be revealed.

B-4. *Cyberspace* is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, embedded processors, and controllers (JP 1-02). The Army operates in and through the cyberspace domain, using and managing the electromagnetic spectrum as a holistic and integrated part of unified land operations. Personnel engaging in OSINT exploitation need to understand the cyberspace environment in order to develop and identify outcomes-based, integration-focused, and resource-informed solutions for cyber situational awareness concerns.

B-5. *Cyber situational awareness* is the knowledge of friendly, neutral, and threat relevant information regarding activities in and through cyberspace and the electromagnetic spectrum (FM 1-02). Cyberspace and cyber security involve increasing cyber situational awareness by—

- Identifying threat operations to determine the effect on friendly operations and countermeasures.
- Determining how to use cyberspace to gain support from friendly and neutral entities.
- Determining how to gain, maintain, and exploit technical and operational advantages.

B-6. There are OPSEC and computer security risks to searching and interacting with Internet Web sites. Searching the Internet can compromise OPSEC by leaving "digital footprints" on visited Web sites. "Surfing" on Internet Web sites can compromise computer security by exposing the computer and network to malicious software (such as viruses, worms, and Trojan Horses) or unauthorized access. Intelligence personnel must be vigilant to potential threats, use only authorized hardware and software, and comply with established unit operations security measures.

B-7. URL information from the previous Web site visited is frequently an OPSEC issue and it identifies characteristics and interests of the user. While necessary for an effective research, the use of specific and focused search terms have potential OPSEC implications.

Cyber Security Example

If the user enters the search terms [bradley us army], the referring URL from the Google hit list would be: http://www.google.com/search?hl=en&q=bradley+us+army. This tells the visited site that the user is searching in English (hl=en) for information on Army General of the Army Omar N. Bradley or the U.S. Army's Bradley infantry fighting vehicle.

B-8. All actions on a Web site are logged and saved. The information is saved and linked to what is referred to as *cookie data*. User actions include but are not limited to—

- Words typed in search parameter fields.
- Drop-down menu choices.
- Check boxes.
- Web site movement patterns such as changing domain name or Web site address.

B-9. On many Web sites, information that the user provides or fills in becomes part of the Web site and is searchable. Key information to avoid sharing includes but is not limited to—

- Military plans.
- Operations.
- Exercises.
- Maps and charts.
- Locations.
- Schedules.
- Equipment vulnerabilities, capabilities, and shortfalls.
- Names and related numbers:
 - Telephone numbers.
 - Birth dates.
 - Identification numbers.

B-10. Traditional and irregular threats are disruptive in nature and use the cyberspace domain to conduct operations against the Army. These threats are innovative, networked, and technologically adept. These threats capitalize on emerging technologies to establish and maintain a cultural and social advantage leveraging areas, to include but not limited to mission command, recruiting, logistics, fund raising and laundering, IO, and propaganda.

B-11. When engaged in OSINT exploitation utilizing computer systems and Internet usage, cyberspace awareness assessments should be developed and cover areas including but not limited to network vulnerabilities, network threats (physical and virtual), and future risks.

B-12. For more detailed information about cyber security threats and tips see the U.S. Computer Security Readiness Team's Web.

Appendix C

Basic and Advanced Internet Search Techniques

The ability to search the Internet is an essential skill for open-source research and acquisition. The Internet, considered a reconnaissance and surveillance research tool, provides access to Web sites and databases that hold a wide range of information on current, planned, and potential areas of operation. The exponential growth in computer technology and the Internet has placed more publicly available information and processing power at the fingertips of Soldiers than ever before. A body of knowledge on culture, economics, geography, military affairs, and politics that was once inaccessible to some degree, now rest in the hands of high school and college students—future leaders of the Army.

THE WORLD WIDE WEB AND DEEP WEB

C-1. The Internet is a dynamic information environment consisting of stationary and moving virtual and target Web sites containing a mixture of old and new content. There are numerous virtual databases that grow at exponential rates. Keeping pace with technology is an enduring challenge for personnel that engage in OSINT exploitation utilizing the WWW and Deep Web.

WORLD WIDE WEB

C-2. The WWW is indexed by standard search engines. Standard search engines are typically incapable of accessing or retrieving the type of information necessary for conducting effective open-source research. The total amount of Internet information is estimated to be over 7,500 terabytes and continues to increase. Of this amount, customary search engines on the Internet are estimated to index only one-quarter of the information. Considered a very large amount of information, it only represents a fraction of the amount of open-source information available during research utilizing publicly available information. The other three-quarters (or roughly 5,625 terabytes) are contained on what is called the Deep Web.

THE DEEP WEB

C-3. The *Deep Web* refers to content that is not part of the traditional WWW. This content is estimated to be more than twice the content saved and accessible on the traditional WWW. The content and information contained on the Deep Web is designed around Web-based databases. Unlike the WWW, the Deep Web is not indexed. Nonstatic Web sites and databases located on the Deep Web cannot be accessed or indexed by traditional search engines. The Deep Web offers a tremendous amount of resources. Deep Web resources could fall into one or more of the following:

- **Dynamic content.** Web pages that are returned in response to a submitted query.
- **Unlinked content.** Web pages that are not linked to other Web pages that prevent standard Web crawling programs from accessing the content.
- **Private Web content.** Web pages without backlinks or inlinks.
- **Limited access content.** Web sites that limit access to information.
- **Nonhypertext markup language content.** Textual content encoded in multimedia files that are not handled by search engines.

SEARCH ENGINES

C-4. Search engines are the primary tools that personnel engaging in OSINT activities use when conducting research of publicly available information through open sources. OSINT personnel use search engines and search terms to locate text, images, and information on thousands of Web sites. Technically, search engines are actually searching through the index of Web sites. Commercial and government search engines vary in what parameters are searched, how searches are processed, and how search results are displayed. Most search engines use programs called *web crawlers* to build indexed databases. A web crawler searches Internet Web sites and files and saves the results in a database.

C-5. Most search engines use relevancy formulas to display results in a specific order with a brief description and hyperlink to the reference Internet file. Relevancy formulas evaluate how well the query matches the request. Relevancy formulas are significant to the user as search engines evolve and will not all yield similar results. The placement of keywords yield different results if rearranged due to more emphasis placed on one word over another. As search engines have evolved, some have become adept at finding specific types of information, such as statistical, financial, and news, more effectively. To overcome this specialization, software engineers have developed metasearch engines that allow the user to query more than one search engine at a time.

Search Engines

If a particular search engine cannot accommodate phrases in quotation marks or other types of Boolean functions, then the metasearch engine eliminates that function from the search. The resulting search then becomes too broad and less useful than a well-formatted search using a specialized search engine.

C-6. With an understanding of how search engines work, intelligence personnel—

- Conduct initial searches using unique keywords and combinations.
- Apply Boolean logic to improve search parameters.
- Conduct follow-on searches using natural language.

SEARCH BY KEYWORD

C-7. In keyword-based searches, OSINT personnel should consider what keywords are unique to the information being researched. Keywords should be balanced to yield relevant results without an over abundance of irrelevant information. Common words to be avoided include—

- A.
- An.
- And.
- The.

C-8. These words should be avoided in search terms unless part of the title of a book or article. Most search engines ignore common words. For example, if looking for information about Russian and Chinese tank sales to Iraq, do not use *tank* as the only keyword in the search. Instead, use additional defining words such as "Russian Chinese tank sales Iraq."

BOOLEAN LOGIC OPERATORS, CONNECTORS, AND DELIMITERS

C-9. When searching the Internet, the vast data available can be searched according to the rules of computer database searches. The logical relationship between search terms is referred to as *Boolean logic*. This method of searching provides options for constructing logical relationships among search terms using local operators, connectors, and delimiters.

C-10. Boolean logic operators, connectors, and delimiters assist intelligence personnel in establishing relationships between keywords to improve search activities.

Example of Using Boolean Logic Operators

Applying the following example, using the operators (see table C-1), the search engine searches for *Russian* and *tank* together when placed within parentheses—for example, *(Russian tank)*—and to exclude Chinese tank sales from the search result, use *(Russian tank) NOT (Chinese tank) sale Iraq* in the search. Intelligence personnel can also use a *NEAR* search when the relationship and the distance between the terms are well established. For example, if intelligence personnel are looking for incidents of tank sales in Baghdad and news articles normally place the name of the location within five words of *tank sales* in the title of the body of the article then use *tank sales NEAR/5* in the search.

Table C-1. Boolean logic operators, connectors, and delimiters

Function	*Boolean*	*Example*
Must be present *	AND	Chemical AND weapon chemical *weapon
Must not be present	NOT	Africa NOT Sudan
May be present	OR	Chemical OR biological
Complete phrase	* *	*Chinese tank sales to Iraq*
Nested	()	(Shining Path)
Near**	NEAR	"White House" NEAR "airspace incursion"
Wildcards	Word* or *word	Gun* (gunpowder)

Note. Boolean searches may not work on all search engines. Using the "Advanced Search" option is available on many web browsers. Advanced search pages include fields to fill in such as "Find web pages that contain all these words;" "this exact wording or phrase;" or "Do not show pages including any of these words."

SEARCH IN NATURAL LANGUAGE

C-11. An alternative to using a keyword search is the *natural language* question format as most of the major search engines allow this capability. OSINT personnel obtain the best results when the question contains good keywords. One of the major downsides to this technique is the large number of results. If the needed information is not found in the results of the first few pages the question should be refined to initiate a new search using different parameters.

INTERNET WEB SITES

C-12. The four steps used to exploit publicly available information and open sources on Internet Web sites are—

- Plan Internet search.
- Conduct Internet search.
- Refine Internet search.
- Record results.

PLAN INTERNET SEARCH

C-13. OSINT personnel use an understanding of intelligence and information requirements to plan Internet searches. Intelligence and information requirements help to determine what information to search for, where to search, and provides the focus and initial keywords used in the search. After determining the focus and keywords, OSINT personnel use Internet browsers and search engines to connect to a previously identified Internet Web site.

Keyword Searches

If a unit is planning a humanitarian assistance operation in a particular country, intelligence requirements may be to locate refugee concentrations in that country. The task for an OSINT cell could include to locate—

- Humanitarian relief organizations operating food distribution centers.
- Population centers in the country.
- Concentrations of militia forces.
- Areas of militia operations within in the last 30 days.

Useful search terms would include—

- Refugee.
- Humanitarian relief.
- Militia.
- Water sources.
- Food distribution.

Locating possible indicators of where refugees may or may not concentrate include—

- Nongovernmental organization aid centers.
- Food.
- Water.
- Hostile militia forces.

Based on intelligence requirements, the search objective is to locate refugee concentrations based on the position of supplies and militia forces in the country.

CONDUCT INTERNET SEARCH

C-14. OSINT personnel conduct an initial search of likely sources using related terms or subject matter for the research question. The initial search is the first of potentially many subsequent searches for data and information that is retrieved and recorded in accordance with the research plan. Once retrieved, the information is integrated into the appropriate digital or analog database. OSINT personnel should avoid the temptation of using only one search engine as each has strengths and weaknesses. Organizational standards, research experience, and peer recommendations typically guide the selection of which search engine to use.

Note. If the information is not identified using multiple search engines within 30 minutes, it is possible that the information does not exist on the Internet, has not been indexed, or is not in a retrievable format.

REFINE INTERNET SEARCH

C-15. Typically, the first few pages of search results are the most relevant. Based on these pages, OSINT personnel exploit the initial search results for relevancy and accuracy for follow-on searches to determine if the results satisfied the intelligence or information requirement. Initial Internet searches can yield undesired results to satisfy intelligence and information requirements. OSINT personnel typically use measures to refine Internet results, including but not limited to—

- Reordering search terms.
- Adjusting upper or lower case.
- Searching within results.
- Searching in the cache and archive.
- Web site domains.
- Changing spelling and grammar.
- Using keyword variants.
- Searching by field.
- Truncating the URL.

Reorder Search Terms

C-16. Search engines may place a higher value on the first word or words in a multiple word or phrase search string. For example, changing the word order from *devices explosive* to *explosive devices* may yield different search results.

Change Spelling and Grammar

C-17. Search engines attempt to match the exact spelling of the words in the search string. There are search engines that recognize alternate spellings or prompt the user to correct common misspellings. For example, changing the spelling of a word from the American-English *center* to the British-English *centre* may yield different results. Boolean logic can also be used in order to circumvent potential spelling mistakes. Additionally, changing the spelling of a transliterated name generates different results that may be useful depending upon the objective of the search, such as the spelling variations of the name—

- *Al-Qaeda*.
- *al-Qaida*.
- *al-Qa'ida*.
- *el-Qaida.*
- *al Qaeda.*

Adjust Upper or Lower Case

C-18. Search engines may or may not support case sensitive searches. Some search engines attempt to match the word exactly as entered in the search. Most searches should be all lowercase letters. When looking for the name of a person, geographical location, title, or other normally capitalized word, use a case sensitive search engine. For example, changing the case of a word such as *java* to *JAVA* changes the results from coffee Web sites to software program Web sites.

Use Keyword Variants

C-19. OSINT personnel use terms that are culturally or geographically common. Using variants of a keyword such as changing *policeman* to *cop*, *bobby*, *gendarme*, *carabiniere*, *policía*, *politzei*, or other forms may improve search results.

Search Within Results

C-20. If the initial or follow-on search produces good but still unsatisfactory results, OSINT personnel can search within these results to produce a higher probability of finding the desired results. Most search engines display an option such as *search within these results* or *similar pages* to assist the user.

Search by Field

C-21. In a field search, OSINT personnel look for keywords within the URL as opposed to searching the Internet. This is typically done when the search engine returned a large number of results. While capabilities vary by search engine, some of the common field search operators are—

- **Anchor.** Searches for Web sites with a specified hyperlink.
- **Domain.** Searches for specific domains.
- **Like.** Searches for Web sites similar or related in some way to specified URLs.
- **Link.** Searches for specific hyperlinks embedded in a Web site.
- **Text.** Searches for specific text in the body of the Web site.
- **URL.** Searches for specific text in complete Web site addresses.

Search in Cache and Archive

C-22. Sometimes a search or an attempt to search with results returns a URL that matches exactly the search objective but when accessed the Web site is no longer active. If the search engine captures data as well as the URL locator, select the cached link to access the original data. OSINT personnel can also search an Internet archive Web site, such as www.archive.org, for the content. OSINT personnel need to have awareness that this information is historical and not subject to update by original creators.

Truncate the Uniform Resource Locator

C-23. Based on the topic of the information or intelligence requirement, OSINT personnel can manually search within the results by truncating the URL to a Web site. OSINT personnel work backwards from the original search result to the Web site containing the desired information or database by deleting the end segments of the URL at the forward slash. See manually truncating a URL example in table C-2.

C-24. There are also URL shortening assistance Web sites that redirect a user from a short URL (such as in the second part of table C-2) to a much longer URL serving as the actual address of the Web site. These are often used in social media services like Twitter due to the character restrictions placed on users.

Table C-2. Truncating and shortening uniform resource locators

Manually Truncating a Uniform Resource Locator (URL)	
Example URL to truncate	http://www.website.com/default.aspx?utm_source=twitter&utm_medium=social-media
Delete all but the main part of the Web site address	http://www.website.com/
Shortening URLs Using Shortening Assistance	
Example URL to paste into shortening assistance Web site	http://www.amazon.com/Kindle-Wireless-Reading-Display-Globally/dp/B003FSUDM4/ref=amb_link_353259562_2?pf_rd_m=ATVPDKIK X0DER&pf_rd_s=center-10&pf_rd_r=11EYKTN682A79T370AM3&pf_rd_t=201&pf_rd_p=1270985982&pf_rd_i=B002Y27P3M
The shortening Web site produces the example URL to use in social media settings or in e-mail	http://tinyurl.com/KindleWireless

Web Site Domains

C-25. Domain names on the Internet are identifying labels and are used in various networking contexts. They are used as simple identification labels to indicate ownership or control of a resource. With the millions of URLs on WWW, intelligence personnel are faced with a myriad of Web sites that may or may not produce or maintain the information presented in that domain. Certain domains, such as those listed in table C-3, are consistently reliable as being administered and authored by those types of organizations.

Note. OSINT personnel exploiting publicly available information and open sources must not take *.org*, *.info*, or *.net* extensions as necessarily produced by a bona fide organization for that domain.

Table C-3. Common Web site domains

Domain	*Description*
.aero	Reserved for members of the air transport industry
.biz	Restricted to businesses
.com	Unrestricted top-level domain intended for commercial content
.coop	Reserved for cooperative associations
.edu	Reserved for postsecondary institutions accredited by an agency on the U.S. Department of Education's list of Nationally Recognized Accrediting Agencies
.gov	Reserved exclusively for the U.S. Government
.info	Unrestricted top-level domain
.int	Used only for registering organizations established by international treaties between governments
.jobs	Reserved for human resource managers
.mil	Reserved exclusively for the U.S. military
.museum	Reserved for museums
.name	Reserved for individuals
.net	Reserved for networking technological individuals
.org	Intended for noncommercial use but open to all communities
.pro	Restricted to credentialed professionals and related entities

OPEN-SOURCE DATABASES, SOFTWARE, AND TOOLS

C-26. There are numerous COTS software applications, tools, and databases that are searchable using query words for research. Search engines used for research include but are not limited to—

- **Google Scholar.** Google Scholar provides a simple way to broadly search for scholarly literature. From one place, searches expand across many disciplines and sources that include articles, theses, books, and abstracts. Google Scholar helps locate relevant work across the world of scholarly research.
- **Spokeo.** Spokeo specializes in organizing people-related information (names, addresses, phone numbers) from phone books, social networks, marketing lists, business Web sites, and other public sources. Spokeo uses algorithms to piece together data into coherent profiles.
- **Blog Pulse.** BlogPulse is an automated trend discovery system for blogs by applying machine-learning and natural language processing techniques.
- **Pipl.** Pipl query engine helps locate Deep Web pages that cannot be found on regular or standard search engines. Pipl uses advanced language-analysis and ranking algorithms to retrieve the most relevant information about an individual.
- **Monitter.** Monitter is a browser-based Twitter search engine. Monitter displays three constantly updated keyword searches parallel to each other in your browser.
- **Maltego.** Maltego is a forensic application that offers data-mining and gathering of information into packaged representations. Maltego allows the identification of key relationships between information and identify previously unknown relationships.

GOOGLE TOOLS

C-27. Google tools assist in exploiting publicly available information and open sources through—

- Query words.
- Query types.
- Query modifiers.

QUERY WORDS

C-28. Google supports several advanced Boolean logic operators, which are query words that have special meaning to Google. Typically query types and query modifiers, when applied by operators, modify the parameters and results of search engines.

QUERY TYPES

C-29. Four categories covering most Web-search queries include—

- **Cache.** If other words are included in the query, Google highlights those words within the cached document. For example, [cache:www.google.com web] shows the cached content with the word "web" highlighted.
- **Link.** The query [link:] lists Web pages that have links to the specified Web page. For example, [link:www.google.com] lists Web pages that have links pointing to the Google homepage.
- **Related.** The query [related:] lists Web pages that are similar to a specified Web page. For example, [related:www.google.com] lists Web pages that are similar to the Google homepage.
- **Info.** The query [info:] presents some information that Google has about that Web page. For example, [info:www.google.com] shows information about the Google homepage.

QUERY MODIFIERS

C-30. Research using a specific search query can be modified using the following modifiers:

- **Site.** If [site:] is included in the query, the results are restricted to those Web sites in the given domain. For example, [help site:www.google.com] finds pages about *help* within www.google.com. [help site:com] finds pages about *help* within *.com* URLs.
- **Allintitle.** If a query starts with [allintitle:], the results are restricted to those Web sites with all of the query words in the title. For example, [allintitle: google search] returns only documents that have both *google* and *search* in the title.
- **Intitle.** If [intitle:] is included in the query, the results are restricted to documents containing that word in the title. For example, [intitle:google search] returns documents that have the word *google* in their title, and have the word *search* anywhere in the document (title or not). Putting [intitle:] in front of every word in the query is equivalent to putting [allintitle:] at the front of the query: [intitle:google intitle:search] is the same as [allintitle: google search].
- **Allinurl.** If a query starts with [allinurl:], the results are restricted to those Web sites with all of the query words in the URL. For example, [allinurl: google search] returns only documents that have both *google* and *search* in the URL.
- **Inurl.** If [inurl:] is included in the query, the results are restricted to those documents containing that word in the URL. For example, [inurl:google search] returns documents that have the word *google* in their URLs, and have the word *search* anywhere in the document (URL or not). Putting "inurl:" in front of every word in the query is equivalent to putting "allinurl:" at the front of the query: [inurl:google inurl:search] is the same as [allinurl: google search].

INTERNATIONAL INTERNET WEB SITES

The number of non-English-language users on the WWW and Deep Web are increasingly surpassing English users. This international reach results in the creation of foreign Web sites with specific country

codes. OSINT personnel must be aware of the origin of foreign Web sites and the potential vulnerabilities inherent in accessing these Web sites.

INTERNET SEARCH TECHNIQUE CONSIDERATIONS

C-31. When conducting Internet basic and advanced searches, technique areas that should be considered are—

- **COTS software.** When utilizing COTS tools and software, OSINT personnel must consider the tools and software utilized in accordance with unit SOPs, guidelines and policies.
- **Cataloging and archiving.** Due to the nature of Internet Web sites and the lack of control restrictions, Web sites can be removed from the WWW without prior notice.
- **Authorship.** Open-source products can oftentimes be authored through anonymity.
- **Identified Web sites and portals.** Familiarization of publicly available information generally results in standardized Web sites and portals used for research. Web sites and portals are subjective in nature due to the biases and perceptions of the Web site administrator or designer.
- **Off-line browsers.** Due to the volatile and unpredictability of Web sites, effective use of off-line browsers can enhance Internet research.

INTERNET AND OPERATIONS SECURITY VULNERABILITIES

C-32. The intent of OSINT is to exploit publicly available information and open sources without revealing user or organizational identities. Exploiting publicly available information and open sources is typically anonymous and conducted with a low risk of potential OPSEC compromise. There are inherent threats when conducting research on the WWW and Deep Web. Open-source research can compromise OPSEC and reveal user identification and the location of the computer systems through IP addresses. Any number of system disruption tools can render open-source collection activities ineffective. These include but are not limited to—

- **Viruses.** Computer codes that attach to computer programs. Once attached, viruses infect other computer systems through replication.
- **Trojan horses.** Computer programs that prevent user-activated commands.
- **Worms.** Self-contained computer programs that infect computers through replication. Worms create traffic on Web sites with the objective of decreasing visibility by conducting denial of service attacks.

Note. OSINT personnel should consult with organic unit's S-6/G-6 and information assurance personnel for current threats and guidelines to ensure that operating systems and browsers are using the most current security patches, antivirus, and antispyware protection software.

Appendix D

OSINT Contributions

The vignettes and discussions in this appendix illustrate how integrated OSINT supports or contributes to—

- Unified land operations and associated missions and tasks.
- Other intelligence disciplines.
- Other functions, such as site exploitation (SE) and source vetting.

The examples provided do not constitute a comprehensive list.

SUPPORT TO TARGETING, COUNTERINSURGENCY, AND IMPROVISED EXPLOSIVE DEVICE DEFEAT OPERATIONS

D-1. As a result of target development, OSINT contributes to the products such as target lists, target folders, target briefs, and exploitation requirements. The following vignette describes one situation where OSINT contributes to targeting. (For more information on targeting see FM 3-60.)

Example of OSINT Contributions to Targeting

The United States is going to war against Country X. The United States has an objective to limit the counterstrike capabilities of Country X. There is a significant military stockpile that Country X purposely collocated by a religious center. Should the United States destroy the stockpile knowing there is a great chance that the symbolic religious center will be destroyed as collateral damage?

OSINT can support this objective by providing information such as—

- What is the religious background of the population living near the religious center?
- Is the religious center culturally significant?
- Is it an historical landmark?
- What is the makeup of the congregation?
- What are the normal times that people congregate?
- What are the technical descriptions of the equipment in the stockpile?

D-2. In support of counterinsurgency operations, publicly available information is valuable for understanding the operational environment. It is often more useful than any other discipline for understanding public attitudes and public support during counterinsurgency operations. Publicly available information is also an important means of determining the effectiveness of inform and influence activities among the local populace. Monitoring public media benefits counterinsurgency operations. If possible, monitoring should occur at every echelon in support of PIRs. Each echelon should monitor the media that contain information relevant to operations at that echelon. For instance, at the corps level, major news networks should be monitored; in contrast, at the tactical level, local newspapers or radio stations may be more important. (For additional information on counterinsurgency operations, see FM 3-24.)

D-3. In support of improvised explosive device (IED) defeat operations, publicly available information can be used to—

- Collect and monitor IED-related information discussed during events that are open to the public or occur in public areas.
- Collect and monitor IED-related information that is located in any recorded public document (such as newspapers, magazines, leaflets, brochures, posters).
- Collect and monitor IED-related information that is broadcast for general public consumption to all receivers or terminals within a computer, radio, or television network.
- Monitor threat or IED-related Internet Web sites that may provide indications and warning of threat intentions, capabilities, activities, and responsible entities for a specific incident.

D-4. See FM 3-90.119 for more information on combined arms IED defeat operations.

SUPPORT TO OTHER INTELLIGENCE DISCIPLINES

D-5. Publicly available information and open sources developed as finalized OSINT can also support other intelligence disciplines.

HUMAN INTELLIGENCE

D-6. OSINT supports HUMINT collection operations by providing open-source materials to the appropriate J/G/S-2X and intelligence community agencies and liaison officers. These materials include but are not limited to—

- Maps.
- Charts.
- Phone directories.
- Business directories.
- Newspapers.
- Video and audio media (including tapes and CDs).

D-7. For further information on HUMINT collector operations see FM 2-22.3.

SIGNALS INTELLIGENCE AND GEOSPATIAL INTELLIGENCE

D-8. The following vignette describes a specific situation where OSINT directly contributes to signals intelligence (SIGINT) and geospatial intelligence (GEOINT).

Example of OSINT Contributions to SIGINT

The signals officer for Unit C is preparing an assessment based on an upcoming operation. The signals officer does not have access to classified systems. Unit C is preparing to conduct operations in an area where the media is state-controlled by a totalitarian government.

OSINT can support the signals officer by providing information such as—

- The identification of locally televised channels along with supporting components and systems.
- Web sites used to communicate to the local populace.

Example of OSINT Contributions to GEOINT

During mission planning, Engineer D is observing the potential effects of building a new rail system. The rail system will bisect an agricultural community located along a primary irrigation path. There is an increased potential that the rail system will disrupt and cause damage to the irrigation canals. There are time constraints preventing the request of satellite imagery in order to provide an overhead view of the area for assessment. If the rail system damages the irrigation canals, the results will more than likely destroy relationships established between unit leadership and tribal leaders.

OSINT can support imagery intelligence (IMINT) by providing information such as Google Earth and other COTS imagery to identify alternative waterways, future irrigation draining areas, and water paths in the event of flooding.

TECHNICAL INTELLIGENCE AND COUNTERINTELLIGENCE

D-9. Publicly available information supports technical intelligence (TECHINT) efforts in significant ways. Although adversaries and potential threats attempt to closely protect capabilities and vulnerabilities as well as intent, the inevitable results of technological advances, such as the Internet and Google Earth, provide exploitation opportunities into even the most secretive nations and organizations. (For further information on TECHINT, see TC 2-22.4.)

D-10. In support of CI, publicly available information can be used to obtain information that satisfies PIRs or other standing CI collection requirements. The collectors of Army OSINT are the military intelligence brigades. Military intelligence Soldiers receive OSINT training at their schools, as applicable. Upon arrival at permanent duty stations, unit training should include OSINT training relevant to duty assignments. (For more information on CI, see FM 2-22.2.)

Appendix E

OSINT Organizations

OSINT expands the entire breath of the intelligence community from the national level to the tactical level of operations. U.S. Government organizations, such as DOD, law enforcement agencies, and others that collect, acquire, exploit, analyze, disseminate, or utilize OSINT as a customer include—

- Defense Open Source Council (DOSC).
- INSCOM.
- DA IIS.
- DNI OSC.
- Open Source Academy.
- ASD.
- FBI.
- Federal Research Division (FRD), Library of Congress.

DEFENSE OPEN SOURCE COUNCIL

E-1. The DOSC is the primary governance mechanism for DOD OSINT. It serves as a forum for the coordination and facilitation of OSINT activities and programs for all Services and combatant commands. The DOSC advices and reports to the Under Secretary of Defense for Intelligence (USD[I]) on OSINT issues and recommends initiatives to improve the effectiveness and efficiency of OSINT programs, activities, and systems of the DOD. The responsibilities of the DOSC include but are not limited to—

- The coordination of activities and the resolution of OSINT programs and activities.
- The prioritization of OSINT requirements.

U.S. ARMY INTELLIGENCE AND SECURITY COMMAND

E-2. INSCOM conducts multidiscipline and all-source intelligence operations to include collection, analysis, production, and dissemination; knowledge management for the Army intelligence enterprise; as well as delivers specialized quick reaction capabilities, advanced skills training, and linguist support for deploying forces to enable battle command to support unified land operations.

E-3. INSCOM regionally supports each of the geographic combatant commands through subordinate regionally focused multifunctional military intelligence brigades. Each brigade manages intelligence requirements (to include OSINT) and provides support to Army tactical units deploying to or operating within a unified combatant command's area of responsibility or operational environment. Each multifunctional brigade has the capability to produce OSINT, generate requests to higher agencies, and answer collection requirements submitted by subordinate units at the tactical level through OSCAR-MS.

DEPARTMENT OF THE ARMY INTELLIGENCE INFORMATION SERVICE

E-4. DA IIS provides a broad spectrum of intelligence support functions to Army and intelligence community customers. DA IIS is the primary OSINT information and dissemination proponent for the Army. DA IIS is an element of Army G-2, Intelligence Information Management Directorate (DAMI-IM) and operational control is assigned to the INSCOM G-3. DA IIS is the primary intelligence information dissemination office for the Army. DA IIS provides a broad spectrum of intelligence support functions to Army and intelligence community customers, including Army Open-Source Collections Requirements Management.

E-5. The mission of the DA IIS is to coordinate, disseminate, and validate the strategic-level requests for open-source requirements Army-wide under the direction of the Army G-2. This is done by providing information sharing services across the intelligence community. The DA IIS is a voting member of the Office of the Director of National Intelligence (ODNI) NOSC Collection Requirements Management (CRM) subcommittee. DA IIS is the Army proponent office for OSINT. As such it addresses all aspects of OSINT policy, training, operational support, collection, production, analysis, and dissemination.

DIRECTOR OF NATIONAL INTELLIGENCE OPEN SOURCE CENTER

E-6. The DNI OSC supports the NOSE as directed by the ADDNI/OS. The OSC is an organization within the intelligence community, U.S. Government, private sector, and academia.

E-7. The operations of the OSC are driven by standing open-source requirements contained in the OSC's annually reviewed and approved information collection plans. The OSC maintains a worldwide network of multilingual regional experts that respond to intelligence and information requirements using publicly available information and open sources such as radio, television, newspapers, news agencies, databases, and the Internet. The OSC monitors open sources in more than 160 countries in over 80 languages and acquires open-source data worldwide for organizations across DOD, U.S. government agencies, and local law enforcement departments.

E-8. OSC services and tools facilitate OSINT efforts of agencies and offices throughout the U.S. Government and intelligence community by enabling the creation, management, and dissemination of unclassified products. The effectiveness and adaptability of OSC tools are—

- Highly developed for open-source exploitation and product creation.
- Designed to support and provide resources to a decentralized customer-base mainly through the Internet and readily available, purchased COTS content.
- Consistent with intelligence community security, technical, and metadata standards.

E-9. The OSC analyzes the content and behavior of media and Internet Web sites of nations and other international actors of significant policy interest to the U.S. Government.

OPEN SOURCE ACADEMY

E-10. The Open Source Academy is a leading provider of open-source tradecraft training. As intelligence consumers place a greater value on OSINT, open-source specialists throughout the U.S. Government are turning to Open Source Academy courses (see table E-1) to build open-source skills and to stay abreast of evolving OSINT technologies. The Open Source Academy is building relationships with community leaders across the intelligence community to develop a comprehensive approach to instilling open-source tradecraft skills. The academy hosts participants expanding across DOD, federal agencies, as well as local law enforcement departments.

Table E-1. Open Source Academy curriculum

• Introduction to the Field • Library Resources and Research Techniques • Media Analysis	• Visual Persuasion Methodology Advanced Googling • Audience Resonance Methodology

• Newcomer's Basic Desktop • Open-source Research and Analysis • Orientation to the Open Source Center • OS 101: Open-source Fundamentals • OS 201: Open-source 201 • Open-source Intelligence (OSINT) and the Other Intelligences • Overview of the Open Source Center Collection Requirements Process • Security and Privacy Issues for Internet Users • Smart Research—Partnering with the Library • Temporary Duty Workshop • Tools and Data Sources	• Classification Workshop • Community Digital Audio Video Enterprise (DAVE) System • Creating Multi-media Products • DAVE Executive Overview • Disseminations • Essentials of Open-source Analysis • Field Management • Fundamentals of Open Source Center Textual Production and Operations (PROPS) • Geospatial Analysis: An Introduction • Hidden Universes of Information on the Internet • High-end Workstation Block II 101 • High-end Workstation Block II 201

U.S. ARMY ASIAN STUDIES DETACHMENT

E-11. The ASD is the oldest, largest, and one of the most well-established OSINT activities in DOD that demonstrates the characteristics of sustained OSINT exploitation. The ASD collects, analyzes, exploits, processes, and reports short-to-mid-term analyses of publicly available information on military capabilities, force protection threats, and other operational-level intelligence information on countries, forces, and nonstate actors of interest in the USPACOM area of responsibility. Such requirements include the capabilities, disposition, and readiness of military forces in China, North Korea, and the Russian Far East, as well as defense-related topics throughout South and Southeast Asia. The ASD serves as a model for combatant command-level OSINT exploitation. The ASD workforce consists of Department of the Army Civilians and Army Reserve and National Guard Soldiers who serve as mission managers and editorial staff and Government of Japan-funded foreign nationals who perform all of the collection, analysis, translation, reporting, library, and graphics support functions.

E-12. The mission of the ASD is to collect, analyze, exploit, and report foreign OSINT in response to USPACOM and U.S. Army Pacific taskings and other national-level intelligence requirements. ASD's OSINT collectors, analysts, and reporters accomplish their wide-scope mission through the exploitation of print and Internet media materials.

E-13. ASD personnel extract and compile information into analytical products answering specific taskings received via the OSCAR-MS. The ASD synthesizes and cites open-source references in open-source intelligence report format similar to research papers or essays. ASD's current operations section provides a suite of daily media summary products containing press articles responding to more immediate and time-sensitive requirements for foreign media reflections of U.S. activities and other topics of interest. The services and tools that the ASD provide include but are not limited to—

- OSINT products responding to OSCAR-MS requirements.
- Analytical open-source intelligence reports.
- Daily force protection/situational awareness reports (FPSARs).
- Daily area surrounding Japan open-source intelligence reports (ASJORs).
- Daily situational reports (SITREPs).
- Weekly China and Taiwan Military photos reports.
- Ad hoc reporting as requested by customer in OSCAR-MS.
- OSINT product distribution on NIPRNET, SIPRNET, and JWICS.
- Map collection.
- Media summary reports.

FEDERAL BUREAU OF INVESTIGATION

E-14. The FBI is an agency of the Department of Justice that serves as both a federal criminal investigative body and an internal intelligence agency. The FBI has investigative jurisdiction over violations of more than 200 categories of federal crime.

E-15. The main missions of the FBI are to protect and defend the United States against terrorist and foreign intelligence threats and to uphold and enforce criminal laws. This is done by focusing on specific categories that include but are not limited to—

- Bank robbery.
- Robbery and extortion affecting interstate commerce.
- Drugs.
- Conspiracy.
- Sexual exploitation of minors.
- Mail fraud.
- Bank fraud.
- Fraud by wire, radio, or television.
- Illegal gambling businesses.

E-16. The FBI uses publicly available information through open sources in the areas of counterterrorism, CI, cybercrime, information technology, and forensics. Within the mission scope of the FBI, the services and tools provided include but are not limited to—

- Law enforcement bulletins.
- Crime mapping.
- Statistics (cybercrime, white-collar crime, and violent crime).

FEDERAL RESEARCH DIVISION, LIBRARY OF CONGRESS

E-17. The FRD was organized during World War II to collect and conduct research on captured aeronautical and technical reports on German and Japanese forces. These collections provided insight to future U.S. defensive posture developments and subsequently assisted in the intelligence effort leading to the defeat of the Axis powers.

E-18. The mission of the FRD is to provide directed research and analysis on domestic and international subjects to agencies of the U.S. Government, the District of Columbia, and authorized federal contractors. The FRD conducts open-source research for the U.S. Library of Congress. The services and tools that the FRD provide include but are not limited to—

- Primary research material, including document delivery.
- Foreign language abstracting and translation.
- Annotated bibliographies.
- Organizational and legislative histories.
- Studies and reports.
- Books.
- Military legal resources.
- Country studies.
- Country profiles.
- Terrorism and criminal studies and assessments.

Appendix F

Open-Source Resources

Intelligence personnel have access to vast amounts of information during research. Understanding and awareness of where to begin to look for specific information can be the largest obstacle analysts encounter. The tables in this appendix list some starting reference points for obtaining information that can be developed and produced into finalized OSINT. Table F-1 lists open-source training and resources that are specifically military.

Table F-1. Military open-source training and resources

Intelligence Knowledge Network (IKN):	
IKN is a knowledge management tool that enables intelligence Soldiers worldwide to communicate, collaborate, and investigate. IKN— • Hosts discussion forums. • Serves as a single point of entry to get to U.S. Army Intelligence Center of Excellence (USAICoE) and other intelligence community Web sites. • Hosts a variety of public and private Web applications that support the intelligence community.	
University of Military Intelligence (UMI):	
UMI is the distance learning arm of the military intelligence schoolhouse. From the UMI Web site, military intelligence professionals can access— • Self-paced and reachback training. • The Cultural, Foreign Language Integration Center. • Military intelligence training resources.	
Army Knowledge Online (AKO) Intelligence:	
AKO Intelligence features— • The Intelligence Collaboration Center. • Knowledge Center (documents, FMs, TCs, ATTPs, and others). • Training, agencies, policy, doctrine, and links to other intelligence-related Web sites.	
AKO Open-Source Program:	
AKO Army Open-Source Program features Open-Source— • Events. • Discussion forums. • Links of interest.	• Intelligence products. • Handbooks.
Military Intelligence Library:	***Available via the IKN and Warfighter Forum homepage***
Military Intelligence Library Reference Center includes many databases and resources, such as— • Journals and magazines. • Forms and publications. • Resource guide.	• Historical documents. • Cultural field readings. • Military Intelligence Foreign Language Training Center (MIFLTC).

Table F-1. Military open-source training and resources (continued)

DA IIS Country Research Portal: ***Available via the DA IIS portal from the AKO homepage***
The Department of the Army Intelligence Information Service (DA IIS) Country Research portal has road-mapped and data-mined networks resulting in a one-stop-shop for intelligence information. Some of the links on this Web site include— • Open-source documents such as Early Bird, Terrorism Daily Update, Baghdad Mosquito, Basra Bugle, and others. • Intelligence community. • Combatant commands. • Analyst references. • Foundry program. ***Note.*** Data is accessible through multiple networks to ensure that intelligence consumers have all required information necessary for mission success.
Intelink-U:
Intelink-U is the designated network of the Department of National Intelligence (DNI) for intelligence collaboration. The Intelink-U is— • Managed by the Intelink Management Office. • A joint-use, remotely accessed, and operationally-implemented information service that is used to access and process unclassified, publicly accessible information only. • Provides a protected environment to exchange authorized unclassified, unclassified for official use only, and sensitive but unclassified information among personnel of the DOD. ***Note.*** Access to Intelink-U services is implemented through multiple virtual private networks.
Joint Military Intelligence Training Center:
Armies of the World
Armed Forces of the World ***Note.*** Requires account log in to access the page. Combined Arms Research Library
Center for Army Lessons Learned (CALL)
CALL
Military Operations in Urban Terrain (MOUT)
MOUT
Military Service Intelligence Organizations
U.S. Army Intelligence and Security Command (INSCOM) Office of Naval Intelligence Air Force Intelligence, Surveillance, and Reconnaissance (ISR) Agency Marine Corps Intelligence Activity
Unified Command Intelligence Organizations
U.S. Central Command U.S. European Command U.S. Pacific Command U.S. Southern Command U.S. Africa Command U.S. Air Force Space Command U.S. Special Operations Command U.S. Strategic Command U.S. Transportation Command

Glossary

SECTION I – ACRONYMS AND ABBREVIATIONS

2X	human intelligence and counterintelligence staff element
ADDNI/OS	assistant deputy to the Director of National Intelligence for Open-source
AM	amplitude modulation
AO	area of operations
AR	Army regulation
ART	Army tactical tasks
ATP	Army techniques publication
ATTP	Army tactics, techniques, and procedures
BCT	brigade combat team
CCIR	commander's critical information requirement
CI	counterintelligence
CIA	Central Intelligence Agency
COA	course of action
CONUS	continental United States
COTS	commercial-off-the-shelf
CRM	collection requirements management
DA	Department of the Army
DA IIS	Department of the Army Intelligence Information Service
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DOSC	Defense Open Source Council
DVD	digital video device
EO	executive order
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service
FFIR	friendly force information requirement
FM	field manual
FMI	field manual interim
FRD	Federal Research Division
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-6	assistant chief of staff, signal

G-7	assistant chief of staff, inform and influence activities
G-9	assistant chief of staff, civil affairs operations
GEOINT	geospatial intelligence
HVT	high-value target
ICD	intelligence community directive
IED	improvised explosive device
IIR	intelligence information report
ILR	Interagency Language Roundtable
INSCOM	United States Army Intelligence and Security Command
IO	information operations
IP	Internet protocol
IPB	intelligence preparation of the battlefield
ISP	Internet service provider
JP	joint publication
JWICS	Joint Worldwide Intelligence Communcations System
MDMP	military decisionmaking process
METT-TC	mission, threat, terrain and weather, troops and support available, time available, and civil considerations (mission variables)
MFLT	machine foreign language translation
mm	millimeter
NIPRNET	Nonsecure Internet Protocol Router Network
NOSC	National Open Source Committee
NOSE	National Open Source Enterprise
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OPSEC	operations security
OSC	Open Source Center
OSCAR-MS	open-source collection acquisition requirement management system
OSINT	open-source intelligence
PIR	priority intelligence requirement
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment, and time (operational variables)
S-2	intelligence staff officer
S-3	operations staff officer
S-6	signal staff officer
S-7	inform and influence activities staff officer
S-9	civil affairs operations staff officer
SCI	sensitive compartmented information
SIPRNET	SECRET Internet Protocol Router Network
SOP	standard operating procedure
TCP/IP	transmission control protocol/Internet protocol

TTP	tactics, techniques, and procedures
URL	uniform resource locator
U.S.	United States
USC	United States Code
WWW	World Wide Web

SECTION II – TERMS

esoteric communications

Public statements whose surface meaning (manifest content) does not reveal the real purpose, meaning, or significance (latent content) of the author.

media source analysis

The systematic comparison of the content, behavior, patterns, and trends of organic media organizations and sources of a country.

open source

Any person or group that provides information without the expectation of privacy—the information, the relationship, or both is not protected against public disclosure.

open-source intelligence

The discipline that pertains to intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. (FM 2-0)

private information

Data, facts, instructions, or other material intended for or restricted to a particular person, group, or organization.

publicly available information

Data, facts, instructions, or other material published or broadcast for general public consumption; available on request to a member of the general public; lawfully seen or heard by any casual observer; or made available at a meeting open to the general public.

References

REQUIRED PUBLICATIONS

These documents must be available to the intended user of this publication.

FM 1-02. *Operational Terms and Graphics.* 21 September 2004.

RELATED PUBLICATIONS

These sources contain relevant supplemental information.

AR 11-6. *Army Foreign Language Program*. 31 August 2009.

AR 25-400-2. *The Army Records Information Management System (ARIMS).* 2 October 2007.

AR 27-60. *Intellectual Property*. 1 June 1993.

AR 190-13. *The Army Physical Security Program*. 25 February 2011.

AR 380-5. *Department of the Army Information Security Program*. 29 September 2000.

AR 380-67. *Department of the Army Personnel Security Program*. 9 September 1988.

AR 381-10. *U.S. Army Intelligence Activities*. 3 May 2007.

AR 530-1. *Operations Security (OPSEC).* 19 April 2007.

ATTP 2-91.6. *Tactics, Techniques, and Procedures for Intelligence Support to Site Exploitation.* 27 December 2010.

Carnegie Mellon Software Engineering Institute.

Chatham House.

Department of the Army Intelligence Information Services.

DOD 5240.1-R. *DoD Intelligence Activities.* 1 December 1982.

DODD 5100.20. *National Security Agency/Central Security Service (NSA/CSS).* 26 January 2010.

DODD 3115.12. *Open Source Intelligence (OSINT).* 24 August 2010.

EO 12333. *United States Intelligence Activities.* 4 December 1981.

FM 2-01.3. *Intelligence Preparation of the Battlefield/Battlespace.* 15 October 2009.

FM 2-19.4. *Brigade Combat Team Intelligence Operations*. 25 November 2008.

FM 2-22.2. *Counterintelligence.* 21 October 2010.

FM 2-22.3. *Human Intelligence Collector Operations*. 6 September 2006.

FM 3-24. *Counterinsurgency*. 15 December 2006.

FM 3-55. *Information Collection*. 14 December 2011.

FM 3-60. *The Targeting Process.* 26 November 2010.

FM 3-90.119. *Combined Arms Improvised Explosive Device Defeat Operations.* 21 September 2007.

FM 5-0. *The Operations Process*. 26 March 2010.

FM 6-0. *Mission Command.* 13 September 2011.

FM 7-0. *Training Units and Developing Leaders for Full Spectrum Operations*. 23 February 2011.

FM 7-15. *The Army Universal Task List.* 27 February 2009.

JP 1-02. *Department of Defense Dictionary of Associated Terms*. 8 November 2010.

JP 2-0. *Joint Intelligence.* 22 June 2007.

JP 2-01. *Joint and National Intelligence Support to Military Operations*. 7 October 2004.

JP 3-0. *Joint Operations.* 17 September 2006.

JP 3-35. *Deployment and Redeployment Operations*. 7 May 2007.

JP 3-59. *Meteorological and Oceanic Operations*. 24 September 2008.

JP 3-60. *Joint Targeting*. 13 April 2007.

JP 4-0. *Joint Logistics.* 18 July 2008.

JP 5-0. *Doctrine for Planning Joint Operations*. 20 January 2005.

Lanicci, John M. "Integrating Weather Exploitation into Air and Space Power Doctrine." *Air Power 12, No. 2*. Summer 1998: 52-63.

Library of Congress, Federal Research Division.

Open Source Center.

TC 2-22.4. *Technical Intelligence.* 19 November 2009.

TC 2-33.4. *Intelligence Analysis*. 1 July 2009.

TC 2-91.8. *Document and Media Exploitation.* 6 August 2010.

U.S. Computer Security Readiness Team.

Title 17 USC. *Copyrights*.

Title 18 USC. *Crimes and Criminal Procedure*.

PRESCRIBED FORMS

None.

REFERENCED FORMS

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

Index

Entries are by paragraph number.

A

analysis, 1-2
 intelligence, 2-22
 Internet, 2-19
 media, 4-20
 mission, 1-16, 3-6
 public documents, 2-14
 requirements for, 2-72

C

Chatham House Rule. *See* public speaking forums.

collection, 1-3, 1-7, 3-2
 and analysis, 1-2
 confidential sources, 3-7
 document, 2-14
 foreign media monitoring, 2-57
 information, 1-12
 linguist requirements, 2-49
 machine foreign language translation systems, 2-55
 open sources, 3-7
 technique, 3-8
 U.S. person information, 2-40

cyberspace
 cyber situational awareness, B-6
 defined, B-5

D

databases, 3-12, C-26
 operational information, 2-23
 technical information, 2-23

dissemination
 considerations, 4-49
 digitization, 4-15
 guidelines, 4-42
 media, 4-33
 methods, 4-43
 standards, 4-19
 U.S. person information, A-19

I

information
 collection, 1-12
 evaluate, 4-2
 operations security, 2-41
 publicly available, 1-2, 1-7, 3-1, 4-2
 reliability and credibility, 4-9
 report and disseminate, 4-39

intelligence products, 4-1

Internet
 Boolean logic, C-9, C-29
 cookie data, B-9
 Deep Web, C-3
 international Web sites, C-32
 operations security vulnerabilities, C-35
 publicly available information, C-12
 search engines, C-4
 search, C-15
 truncate the uniform resource locator, C-23
 Web site domains, C-25
 Web sites, 2-19, 3-23
 World Wide Web, C-2

L

legal restrictions
 AR 27-60, 2-48
 AR 381-10, A-7
 copyright, 2-46
 Executive Order 12333, A-1
 fair use, 2-47
 intellectual property, 2-46
 Intelligence Community Directive 300, A-23
 Intelligence Community Directive 301, A-23

M

MDMP, 1-15

media
 analysis, 4-20
 content, 4-35
 control, 4-24
 structure, 4-26

military decisionmaking process. *See* MDMP.

O

open source, 1-1

open-source
 credibility, 2-39
 reliability, 2-34

open-source intelligence. *See* OSINT.

OSINT, 1-1
 and the intelligence process, 1-11
 characteristics, 1-4
 contributions to counterinsurgency operations, D-1
 contributions to GEOINT, D-9
 contributions to HUMINT, D-6
 contributions to improvised explosive device defeat operations, D-1
 contributions to intelligence preparation of the battlefield, 1-18
 contributions to SIGINT, D-9
 contributions to site exploitation, D-12
 contributions to source vetting, D-12
 contributions to targeting operations, D-1
 coordination, 2-44
 deception and bias, 2-45
 defined, 1-1
 exploitation, 2-11, 2-21
 personnel, 2-66
 planning, 2-1
 private information, 3-6
 publicly available information, 3-6

OSINT organizations
 Asian Studies Detachment, 2-28, E-13
 Assistant Deputy Director of National Intelligence for Open Source, A-25
 Defense Open Source Council, E-1
 Department of the Army Intelligence Information Service, E-4

Entries are by paragraph number.

Director of National Intelligence Open Source Center, A-28, E-8
Federal Bureau of Investigation, E-16
Federal Research Division, Library of Congress, E-20
U.S. Army Intelligence and Security Command, E-2
National Open-Source Committee, A-27
Open Source Academy, E-12

P

public broadcasts, 2-17, 3-21
public documents, 2-14, 3-20
public speaking forums, 2-11, 3-18
Chatham House Rule, 3-18

R

requirement
commander's criticial information, 1-13, 3-2
friendly force information, 1-13, 3-2
priority intelligence, 1-13, 3-2
intelligence, 3-5
priority intelligence, 3-2
research, 3-11
field research, 3-13
open-source, 3-1
plan, 3-16
practical, 3-13
question, 3-15

S

security domains, 4-44
Joint Worldwide Intelligence Communications System, 4-46
Nonsecure Internet Protocol Router Network, 4-48
SECRET Internet Protocol Router Network, 4-47
sources
analysis of the media, 4-20
authoritative, 4-10
confidential, 3-7
credibility ratings, 2-39
nonauthoritative, 4-11
open, 1-1, 3-7
primary, 2-35
reliability ratings, 2-38
secondary, 2-37

T

threat
courses of action, 2-8
evaluate, 2-7

U

U.S. person information
collection of 2-40, A-8
dissemination of, A-19
retention of, A-14

ATP 2-22.9
10 July 2012

By order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army

DISTRIBUTION:

Unlimited Distribution; Not to be distributed; electronic media only.



I-INTELLIGENCE

OPEN SOURCE INTELLIGENCE TOOLS AND RESOURCES HANDBOOK

I-INTELLIGENCE

OPEN SOURCE INTELLIGENCE

TOOLS AND RESOURCES HANDBOOK

2018

Aleksandra Bielska

Natalie Anderson, Vytenis Benetis, Cristina Viehman

Foreword

I am delighted to share the latest version of our OSINT Tools and Resources Handbook. This version is almost three times the size of the last public release in 2016. It reflects the changing intelligence needs of our clients in both the public and private sector, as well as the many areas we have been active in over the past two years.

No list of OSINT tools is perfect, nor is it likely to be complete. Indeed, such is the pace of change that by the time you read this document some of our suggestions may have been surpassed or have ceased to exist. Regrettably, today's tool might also be tomorrow's vulnerability.

To counter the first problem, we have included a list of toolkits provided by other OSINT practitioners working to improve the state-of-the-art. To manage the second, we recommend that all tools be tested in a secure computing environment whenever possible.

Work on the next iteration of the Handbook has already begun. For now, I hope this version contributes to improving your efficiency and effectiveness as a researcher, analyst, investigator or general OSINT practitioner. Please feel free to share it with your colleagues. To encourage its broadest possible dissemination, we are publishing the Handbook under a Creative Commons CC BY License.

I would like to end by thanking my colleagues at i-intelligence for their efforts in compiling the Handbook. Particular credit is due to Aleksandra Bielska who led the project and has coordinated the inputs from different contributors. I am also indebted to Natalie Anderson of Mercyhurst University for her excellent research and for the time spent checking these links. Kris Wheaton and Brad Gleason from Mercyhurst's Department of Intelligence Studies are also thanked for their support.

Finally, I would like to thank our community of followers on Twitter for sharing their recommendations with us, as well as the many practitioners who have suggested new tools to us while participating in our courses.

Chris Pallaris
Director, i-intelligence GmbH

CC BY

Table of Contents

Foreword 2

Search 9
- General Search 9
- Meta Search 11
- Visual Search and Clustering Search Engines 12
- National Search Engines 13
- Code Search 16
- FTP Search 17
- Similar Sites Search 18
- IoT Search Engines 19
- Kids-Friendly Search Engines 20
- Other Specialty Search Engines 21
- Other Search Engines and Tools 23

Social Media 25
- Major Social Networks 25
- Real-Time Search, Social Media Search, and General Social Media Tools 27
- Social Media Tools: Twitter 30
- Social Media Tools: Facebook 35
- Social Media Tools: Google+ 37
- Social Media Tools: Instagram 38
- Social Media Tools: Pinterest 40
- Social Media Tools: Reddit 41
- Social Media Tools: VKontakte 43
- Social Media Tools: Tumblr 44
- Social Media Tools: LinkedIn 45
- Social Media Tools: Snapchat 46
- Social Media Tools: WhatsApp 47
- Social Media Tools: Skype 48
- Social Media Tools: Telegram 49
- Other Instant Messaging and Chat Tools 50
- Dating Apps 51

Blogs, Forums, Discussion Boards, and Q&A Sites 52
- Blog Search 52

Forums and Discussion Boards Search 53
Q&A Sites 54

People Investigations 55
Main People Search Tools and Engines 55
Address & Contact Information Search 58
Public Records 60
Ancestry Research 62
Phone Search 63
E-mail Search / E-mail Check 66
Username Check 70
CV and Resume Search 71
Expert Search 72
Salary Search 74
Creating a Sock Puppet 76

Company Research 77
Main Company Search Tools and Engines 77
Company Research (EU) 80
Company Research (UK) 81
Company Research (US) 84
Company Research (Switzerland) 86
Company Research (Middle East) 87
Company Research (Africa) 88
Company Research (China) 90
Business Registers (EU + EFTA) 91
Business Registers (US) 93
Business Registers (Other) 95
Business Registers Lists and Directories 97
Job Search Resources 99
Company Reviews 101
Patent Research 102
Tenders 104
Charity, NGO, and Nonprofit Research 106

Real Estate Research 108
Real Estate Research 108

Online Marketplaces 111
Classifieds and Online Marketplaces 111

Cryptocurrencies and Financial Information 114
Cryptocurrencies 114

Financial Information 115
Legal Research 116
Legal Research Reources and Tools 116
Researching Countries 119
Country Profiles 119
Researching Terrorism, Crime, and Cybersecurity 120
Researching Terrorism 120
Researching Crime 122
Researching Cybersecurity 123
Researching Stolen Items 125
Researching Stolen Items 125
Researching Human Trafficking 127
Researching Human Trafficking 127
Transportation 131
Airplanes 131
Drones 133
Cars 135
Railways 137
Public Transport 141
Ships 144
Container and Cargo Tracking 146
Web Intelligence 147
Domain and IP Research, Websites Analysis 147
Web History and Website Capture 155
Wifi Search 157
Researching Dark Web 158
Researching Dark Web 158
Events Search 160
Events Search 160
Working with Images 161
Image Search and Reverse Image Search 161
Image Analysis 164
Stock Images 167
Image and Photo Editing 169
OCR Tools 171
Working with Videos 172

Video Search and Reverse Video Search 172
Live Streaming and Webcams 174
Other Video Tools 176
Video Editors 179

Working with Audio 181
Radio 181
Podcasts 183
Other Audio Tools 185

Working with Documents 186
Documents and Slides Search 186
Pastebins 188
Document and Reference Management 189
PDF Management 190
Working with Document Metadata 191

Academic Resources and Grey Literature 192
Academic and Grey Literature Research Tools 192

Lectures, Talks, Conference Presentations, Speeches 196
Lectures, Talks, Conference Presentations, Speeches 196

Books and Reading 198
Books Search and Reading Tools 198

Working with Data and Statistics 201
Data and Statistics 201
Infographics and Data Visualization 206
Dashboard Tools 209
Data Analysis 210
Data Scrapers 212

Working with News 214
News Sources 214
News Digest and Discovery Tools 216
Fact Checking 217

Working with Foreign Language Content 219
Translation Tools 219

Web Monitoring 222
RSS Readers 222
Other RSS Tools 224
Website Monitoring 225
Social Media Monitoring 226

Other Monitoring Tools 227

Data Collation 228
Bookmarking 228
Notetaking 231
Annotation and Highlighting 233
Screenshot and Screen Capture Tools 234

Browsing and Browsers 236
Browsers 236
Startpages 238
Customising New Tab 239
Tab Management 241
Extension Managers 243
Offline Browsing 244
Browsing History 245
Other Browsing Tools 246

Writing and Dissemination 247
Writing and Office Tools 247
Slideshow and Presentation Tools 249
Digital Publishing 251
Newsletter Tools 252
Digital Storytelling 253

Wikis, Websites, and Web Apps 255
Wikis 255
Website Builders 256
App Builders 258

Mind Mapping, Concept Mapping and Idea Generation 259
Mind Mapping, Concept Mapping and Idea Generation Tools 259

Productivity and File Management 261
Main Work Management and Productivity Tools 261
E-mail Management 264
Cloud Storage and File Sharing 266
Web Automation 268

Collaboration and Communication 269
Collaboration and Project Management 269
Communication Tools 273

Other Utility Tools 276
File Converters 276

URL Shorteners and Expanders 278
Keywords Discovery and Research 279
Android Emulators 280
Virtual Machine 281
Date & Time 282
Weather 283
Barcodes 285

Analysis 286
Social Network Analysis 286

Geospatial OSINT 287
Geospatial Research and Mapping Tools 287
Interesting Maps 293

Privacy and Security 295
General Privacy Tools and Resources 295
Secure Browsing 297
Ads and Tracking Blockers 301
Blocking of Currency Miners 302
Private Search Engines and Private Searching 303
Secure OS 304
Backup Tools 305
Secure Communication Tools 306
E-mail Security 307
Phone Security 309
Password Management and Secure Login 310
Encryption Tools 311
Secure File Sharing 313
VPN Services 314
VPN Texting 316
Proxy Tools 317
Antivirus Software 318
Other Security Tools 319
Copyright and Takedowns 320
Researching Leaks 321

Research and Recon Tools 322
Research and Data Recon Tools 322

OSINT Tools Lists 324
OSINT Tools Lists 324

Search

General Search

Tool	Link
Aol	http://search.aol.com
Ask	http://www.ask.com
Baidu	http://www.baidu.com
Bing	http://www.bing.com
Deeperweb	http://deeperweb.com
Dothop	http://dothop.com
DuckDuckGo	https://duckduckgo.com
Ecosia	https://www.ecosia.org
entireweb	https://www.entireweb.com
Factbites	http://www.factbites.com
Gigablast	http://gigablast.com
Goodsearch	http://www.goodsearch.com
Google Advanced Search	https://www.google.com/advanced_search
Google Search	http://www.google.com
Jive Search	https://www.jivesearch.com
Lycos	http://www.lycos.com
MyWebSearch	http://home.mywebsearch.com
SurfCanyon	http://www.surfcanyon.com
Teoma	http://www.teoma.com
Wolfram Alpha	http://www.wolframalpha.com
Yahoo! Search	http://www.yahoo.com

Yandex	https://www.yandex.com

Meta Search

Tool	Link
All-in-One	http://all-io.net
AllTheInternet	http://www.alltheinternet.com
Bing vs. Google	http://bvsg.org
Dogpile	http://www.dogpile.com
eLocalFinder	http://www.elocalfinder.com/HSearch.aspx
Etools	http://www.etools.ch
Excite	http://msxml.excite.com
FaganFinder	http://www.faganfinder.com/engines
Findsmarter	http://www.findsmarter.com
Info.com	http://www.info.com
Infospace	http://www.infospace.com
Instya	http://www.instya.com
iZito	http://www.izito.com
Nextaris	http://www.nextaris.com
Metabear	http://www.metabear.com
Monster Crawler	http://www.monstercrawler.com
Myallsearch	http://www.myallsearch.com
opentext	http://fqs.opentext.com/web.htm
Search	https://www.search.com
Sputtr	http://www.sputtr.com
SonicRun	http://www.sonicrun.com
Trovando	http://www.trovando.it
WebCrawler	http://www.webcrawler.com
Zapmeta	http://www.zapmeta.com

Visual Search and Clustering Search Engines

Tool	Link
Answer The Public	https://answerthepublic.com
Carrot2	http://search.carrot2.org
Cluuz	http://www.cluuz.com
Exalead	http://www.exalead.com
iSEEK	http://iseek.com
Yippy	http://yippy.com

National Search Engines

Tool	Link
1ste Keuze (Netherlands)	http://www.eerstekeuze.nl
360 so (China)	https://www.so.com
AEIOU (Portugal)	http://www.aeiou.pt
Alleba (Philippines)	http://www.alleba.com
AnoKato (Greece)	http://www.ano-kato.com
AONDE (Brazil)	http://www.aonde.com
Apali! (Spain)	http://www.apali.com
Arabo (Algeria)	http://www.arabo.com
Arama (Turkey)	http://www.arama.com
Baidu (China)	http://www.baidu.com
Baidu In English	http://baiduinenglish.com
Daum (South Korea)	http://www.daum.net
Deusu (Germany)	https://deusu.de
Dive3000 (Italy)	http://www.dive3000.com/search
Editus.lu (Luxembourg)	https://www.editus.lu
Eniro (Sweden)	http://www.eniro.se
FineLib (Nigeria)	http://www.finelib.com
Finna (Finland)	https://www.finna.fi
Fireball (Germany)	https://fireball.de
Freenet.de (Germany)	http://suche.freenet.de
Goo (Japan)	http://www.goo.ne.jp
Gooru (Poland)	http://www.gooru.pl
Hao123 (China)	https://www.hao123.com
Iranmehr (Iran)	http://www.iranmehr.com

Jamasp (Iran)	http://www.jamasp.ir
KacMac (Syria)	http://www.kacmac.com
Kvasir (Norway)	http://www.kvasir.no
Leit (Iceland)	http://leit.is
Libero (Italy)	http://arianna.libero.it
Lycos.fr (France)	http://www.lycos.fr
Makupalat (Finland)	https://www.finna.fi
Maven Search (Israel)	http://www.mavensearch.com
MetaGer (Germany)	https://metager.de
Mojeek (United Kingdom)	https://www.mojeek.co.uk
Mozbot (France)	https://www.mozbot.com
Najdsi (Slovenia)	http://www.najdi.si
Nate (South Korea)	http://www.nate.com
Naver (South Korea)	http://www.naver.com
Onet.pl (Poland)	http://www.onet.pl
Orange (France)	http://www.orange.fr
Parseek (Iran)	http://www.parseek.com
Pipilika (Bangladesh)	https://www.pipilika.com
Raftaar (India)	https://www.raftaar.in
Raziskovalec (Slovenia)	http://www.raziskovalec.com
Rismoon (Iran)	http://www.rismoon.com
Rootle (Russia)	http://www.rootle.ru
SAPO (Portugal)	http://www.sapo.pt
Search.bg (Bulgaria)	http://www.search.bg
Search.ch (Switzerland)	http://www.search.ch
Search Engine Colossus	http://searchenginecolossus.com
Search Lotto (United Kingdom)	https://www.searchlotto.co.uk
Seznam (Czech Republic)	https://www.seznam.cz
Shamrock (Ireland)	http://www.ireland-information.com/engine
Sina (China)	Https://www.sina.com.cn
Sogou (China)	https://www.sogou.com
Surf (Slovakia)	http://www.surf.sk

Walla (Israel)	http://www.walla.co.il
Yam (Taiwan)	http://search.yam.com
Yandex (Russia)	http://www.yandex.com
Yoodle (Switzerland)	http://www.yoodle.ch
Yooz (Iran)	https://yooz.ir
Vinden (Netherlands)	https://www.vinden.nl
Qq.com (China)	http://www.qq.com
Zoznam (Slovakia)	https://www.zoznam.sk

Code Search

Tool	Link
NerdyData	https://search.nerdydata.com
Google Code Search	https://code.google.com
PublicWWW	https://publicwww.com
Programmable Web	https://www.programmableweb.com
SearchCode	https://searchcode.com

FTP Search

Tool	Link
Archie	http://archie.icm.edu.pl/archie_eng.html
Filemare	https://filemare.com
Global File Search	http://globalfilesearch.com
Global File Search	http://globalfilesearch.net
MMNT	http://www.mmnt.ru
NAPALM FTP Indexer	http://www.searchftps.net

Similar Sites Search

Tool	Link
Find Similar Sites	http://www.findsimilarsites.com
Google Similar Pages	https://chrome.google.com/webstore/detail/google-similar-pages/pjnfggphgdjblhfjaphkjhfpiiekbbej
SimilarPages	http://www.similarpages.com
SimilarSites	http://www.similarsites.com
SimilarSiteSearch	http://www.similarsitesearch.com
SitesLike	http://www.siteslike.com

IoT Search Engines

Tool	Link
Internet of Things Scanner	https://iotscanner.bullguard.com
Shodan	https://www.shodan.io
Thingful	https://www.thingful.net
ZoomEye	https://www.zoomeye.org

Kids-Friendly Search Engines

Tool	Link
Fact Monster	https://www.factmonster.com
KidsClick	http://www.kidsclick.org
KidRex	http://www.kidrex.org
Topmarks	https://www.topmarks.co.uk

Other Specialty Search Engines

Tool	Link
Athlinks	https://www.athlinks.com
Biznar	http://biznar.com
Blade Search	https://bladesearch.com
CiteSeerX	http://citeseer.ist.psu.edu
crunchbase	https://www.crunchbase.com
Datasheet Library	http://www.datasheetlib.com
Digle	https://www.digle.com
Economic Search Engine	http://ese.rfe.org
FluidDATA	https://fluid.bitplatter.com
Google Custom Search	http://www.google.com/cse
Harmari	https://www.harmari.com/search/unified
Instant Logo Search	http://instantlogosearch.com
Internet Archive	https://archive.org/
Lableb	https://lableb.com
moocha	https://www.moocha.io
Open Hub	https://www.openhub.net
Qwikia	http://www.qwika.com
Rebbutter.me	http://rebutter.me
ShareDir	https://sharedir.com
Sweet Search	https://www.sweetsearch.com
SymbolHound	http://symbolhound.com
Think Tank Search	https://guides.library.harvard.edu/hks/think_tank_search
WikiVisually	https://wikivisually.com
WorldWideScience.org	http://worldwidescience.org

Yamli	http://www.yamli.com
Yobi 3D	https://www.yobi3d.com
Zanran	http://zanran.com

Other Search Engines and Tools

Tool	Link
2lingual Search	http://www.2lingual.com
Advangle	http://advangle.com
Answer the Public	https://answerthepublic.com
AOL Search Database	https://search-id.com
Banana SLUG	http://www.bananaslug.com
BOOL	https://chrome.google.com/webstore/detail/bool/cfpmoigmhcehoegokjllchipdiindpkc
Context Menu Search	https://chrome.google.com/webstore/detail/context-menu-search/ocpcmghnefmdhljkoiapafejjohldoga
Custom Search	https://inteltechniques.com/OSINT/user.html
Impersonal.me	http://www.impersonal.me
European Search Engines, Directories and Lists	http://www.searchenginesoftheworld.com/search_engines_of_europe/
Fast Advanced Google Search	https://chrome.google.com/webstore/detail/fast-advanced-google-sear/idijdjdcncjcgmeiipcnkpjedhgepalk?hl=en
Faster Google Search	https://chrome.google.com/webstore/detail/faster-google-search/fmhiafgdfaglfbaaefbbolaholfhkmjc?hl=en
Google Correlate	https://www.google.com/trends/correlate
Google Search Filter	https://chrome.google.com/webstore/detail/google-search-filter/eidhkmnbiahhgbgpjpiimdogfidfikgf?hl=en
Google Similar Pages	https://chrome.google.com/webstore/detail/google-similar-pages/pjnfggphgdjblhfjaphkjhfpiiekbbej
Infinite Scroll	https://chrome.google.com/webstore/detail/infinite-scroll-for-googl/acjdmkdcbbhokaleofmalpcnnkpgphpb?hl=en-US
I Search From	https://isearchfrom.com

Klug Suchen	http://www.klug-suchen.de
Million Short	https://millionshort.com
Net Data Directory	http://netdatadirectory.org
Neuskool	http://neuskool.com
pagodo	https://github.com/opsdisk/pagodo
Polycola	http://www.polycola.com
RESULTER	https://chrome.google.com/webstore/detail/resulter-google-search-sh/chojfhfgbdaeokblbdeahgbijodikdpk
Result Preview	https://chrome.google.com/webstore/detail/result-preview/geogklgaaafmfijgfninjjbcinicfafb
Ruin My Search History	http://ruinmysearchhistory.com
SCANNER-INURLBR	https://github.com/googleinurl/SCANNER-INURLBR
Search by Image	https://chrome.google.com/webstore/detail/search-by-image-by-google/dajedkncpodkggklbegccjpmnglmnflm/related?hl=en
Search Engine Colossus	http://www.searchenginecolossus.com
Search Engines of the World	https://www.searchenginesoftheworld.com
Search Preview	https://chrome.google.com/webstore/detail/search-preview/majhgbekihmliceijipbdccgicepmmei
Search the current site	https://chrome.google.com/webstore/detail/search-the-current-site/jliolpcnkmolaaecncdfeofombdekjcp
Secret Search Engine Labs	http://www.secretsearchenginelabs.com
Selection Search	https://chrome.google.com/webstore/detail/selection-search/gipnlpdeieaidmmeaichnddnmjmcakoe
Sensebot	http://sensebot.com
Suchmaschinen Datenbank	http://www.suchmaschinen-datenbank.de
tracerT	https://github.com/GeneralTesler/tracerT
wiby	https://wiby.me

Social Media

Major Social Networks

Tool	Link
Draugiem (Latvia)	https://www.draugiem.lv
Facebook	http://www.facebook.com
Facenama (Iran)	http://facenama.com
Fediverse	https://fediverse.party
Flickr	https://www.flickr.com
Google+	https://plus.google.com
Instagram	https://www.instagram.com
kik	https://www.kik.com
Linkedin	https://www.linkedin.com
Mastodon	https://mastodon.social
Meetup.com	https://www.meetup.com
Mixi (Japan)	https://mixi.jp
Odnoklassniki (Russia)	http://ok.ru
Periscope	https://www.pscp.tv
Pinterest	http://www.pinterest.com
Qzone (China)	http://qzone.qq.com
Reddit	https://www.reddit.com
Snapchat	https://www.snapchat.com
Swarm	https://www.swarmapp.com
Taringa (Latin America)	http://www.taringa.net
Tinder	https://www.gotinder.com

Tumblr	https://www.tumblr.com
Twitter	https://twitter.com
VKontakte	https://vk.com
Weibo (China)	http://weibo.com
Xing	https://www.xing.com
YouTube	https://www.youtube.com

Real-Time Search, Social Media Search, and General Social Media Tools

Tool	Link
360 social.me	https://www.360social.me
Agora pulse	https://www.agorapulse.com
AIDR	http://aidr.qcri.org
Audiense	https://www.audiense.com
Bloopish	http://bloopish.com
Brand24	https://brand24.com
Brandwatch	https://www.brandwatch.com
Buffer	https://buffer.com
Buzzsumo	http://buzzsumo.com
CrowdTangle Link Checker	https://chrome.google.com/webstore/detail/crowdtangle-link-checker/klakndphagmmfkpelfkgjbkimjihpmkh
Custom Communities Search	https://inteltechniques.com/osint/communities.html
Custom Social Networks Search	https://inteltechniques.com/osint/social.networks.html
Cyfe	http://www.cyfe.com
Falcon	https://www.falcon.io
Flumes	http://flumes.com
Gaddr	https://gaddr.me
Geocreepy	http://www.geocreepy.com \|\| https://n0where.net/creepy
Geofeedia	https://geofeedia.com
Hootsuite	http://hootsuite.com
HowSociable	http://www.howsociable.com
Hashtatit	http://www.hashatit.com

Keybase	https://keybase.io
Keyhole	http://keyhole.co
Klear	http://klear.com
Kred	http://kred.com
ManyContacts Mail Check	https://www.manycontacts.com/en/mail-check
Mention	https://mention.com
MustBePresent	http://mustbepresent.com
netlytic	https://netlytic.org
Netvibes	http://www.netvibes.com
NUVI	https://www.nuvi.com
OpinionCrawl	http://www.opinioncrawl.com
Profilr	https://www.profilr.social/search/jsmith
Pulsar	https://www.pulsarplatform.com
Rival IQ	https://www.rivaliq.com
RSS Social Analyzer	https://chrome.google.com/webstore/detail/rss-social-analyzer/ncmajlpbfckecekfamgfkmckbpihjfdn?hl=en
Samdesk	https://www.samdesk.io
Sendible	https://www.sendible.com
Smaller Social Networks Search	https://inteltechniques.com/osint/smaller.social.networks.html
SocialBakers	http://www.socialbakers.com
SocialBlade	http://socialblade.com
Social DownORNot	http://social.downornot.com
Socialhome	https://socialhome.network
Social Media Monitoring Solutions	http://wiki.kenburbary.com/social-meda-monitoring-wiki
Social Mention	http://socialmention.com
Social Sear.ch	http://www.socialsear.ch
Social Searcher	http://www.social-searcher.com
SproutSocial	https://sproutsocial.com
Storyful Multisearch	https://chrome.google.com/webstore/detail/storyful-multisearch/hkglibabhninbjmaccpajiakojeacnaf?hl=en
Tagboard	https://tagboard.com
Trackur	http://www.trackur.com

UnionMetrics	https://unionmetrics.com
UVRX	http://www.uvrx.com/social.html
Visibrain	https://www.visibrain.com
Webometric	http://lexiurl.wlv.ac.uk
Zoho Social	https://www.zoho.com/social/social-media-monitoring.html

Social Media Tools: Twitter

Tool	Link
AccountAnalysis	https://accountanalysis.lucahammer.com
AllDeletedTweets From Politicians	https://politwoops.com/countries
AllMyTweets	https://www.allmytweets.net/connect
audiense	https://audiense.com
Backtweets	http://backtweets.com
Birdwatcher	https://n0where.net/twitter-osint-framework
Blue Nod	http://bluenod.com
Botcheck.me	https://botcheck.me
Botometer	https://botometer.iuni.iu.edu
Burrrd	https://burrrd.com
BU-TCAT	http://www.bu.edu/com/research/bu-tcat/#left-sidebar
Charm	http://charm.benapps.net
Chorus	http://chorusanalytics.co.uk/chorus/request_download.php
Commun.it	http://commun.it
COSMOS	http://socialdatalab.net/software
Custom Twitter Tools	https://inteltechniques.com/menu.html
Deadbird	https://keitharm.me/project/deadbird
Discover Text	https://discovertext.com
DMI-TCAT	https://github.com/digitalmethodsinitiative/dmi-tcat
doesfollow	https://doesfollow.com
Download Twitter Video	http://www.downloadtwittervideo.com
Echosec	https://app.echosec.net
Fake Follower Check	https://fakers.statuspeople.com

First Tweet	http://ctrlq.org/first
FlipFeed	https://flipfeed.media.mit.edu
Foller.me	http://foller.me
Followerwonk	http://followerwonk.com
Followthehashtag	http://www.followthehashtag.com
GeoSocial Footprint	http://geosocialfootprint.com
Geotweet	http://geotweet.altervista.org
GetTwitterID	http://gettwitterid.com
Gigatweeter	http://gigatweeter.com
HappyGrumpy	https://www.happygrumpy.com
Hashtagify	http://hashtagify.me
Hashtags.org	http://www.hashtags.org
InTweets	http://intweets.com
Jooicer	https://jooicer.com
Keyhole	http://keyhole.co
Klear	https://klear.com
Lakako	https://www.lakako.com/twitter
Lazqa	http://www.lazqa.com
ManageFlitter	http://manageflitter.com
MentionMapp	http://mentionmapp.com
My Twitter ID	http://mytwitterid.com
nowTweets	http://nowtweets.com
OneMillionTweetMap	http://onemilliontweetmap.com
Quarter tweets	http://qtrtweets.com/twitter
Queryfeed	https://queryfeed.net
RiteTag	https://ritetag.com
SaveVideo	http://savevideo.me
Sentiment140	http://www.twittersentiment.appspot.com
Silver Bird	https://chrome.google.com/webstore/detail/silver-bird/encaiiljifbdbjlphpgpiimidegddhic?hl=en
Sleeping Time	http://sleepingtime.org
SnapBird	http://snapbird.org
Social Bearing	http://www.socialbearing.com

Social Rank First Follower	http://socialrank.com/firstfollower
SocioViz	http://socioviz.net
Spoonbill	https://spoonbill.io
tagboard	https://tagboard.com
Tagdef	https://tagdef.com
TAGS	https://tags.hawksey.info
Thread Reader	https://threadreaderapp.com
Tinfoleak	https://tinfoleak.com
Treeverse	https://chrome.google.com/webstore/detail/treeverse/aahmjdadniahaicebomlagekkcnlcila
Trends24	http://trends24.in
TrendsMap	http://trendsmap.com
Twayback Machine	http://staringispolite.github.io/twayback-machine
Twazzup	http://www.twazzup.com
twbirthday	http://twbirthday.com
TwChat	http://twchat.com
TWDOWN	https://twdown.net
TweepDiff	http://tweepdiff.com
Tweeple Search	https://tweeplesearch.com
Tweepsect	http://tweepsect.com
Tweepsmap	http://tweepsmap.com
Tweet Archiver	https://chrome.google.com/webstore/detail/twitter-archiver/pkanpfekacaojdncfgbjadedbggbbphi?hl=en
TweetArchivist	http://www.tweetarchivist.com
Tweetbeaver	https://tweetbeaver.com
Tweet Chat	http://www.tweetchat.com
TweetDeck	https://www.tweetdeck.com
TweeterID	https://tweeterid.com
TweetMap	http://mapd.csail.mit.edu/tweetmap
TweetMap	https://www.mapd.com/demos/tweetmap
Tweet Mapper	https://keitharm.me/projects/tweet
Tweetpaths	http://www.tweetpaths.com
TweetPsych	http://tweetpsych.com

Tweetreach	http://tweetreach.com
Tweets_analyzer	https://github.com/x0rz/tweets_analyzer
TweetStats	http://www.tweetstats.com
Tweet Tag	http://www.tweet-tag.com
TweetTunnel	http://tweettunnel.com
Twellow	http://www.twellow.com
Tweriod	http://www.tweriod.com
Twiangulate	http://www.twiangulate.com
Twicsy	http://twicsy.com
Twilert	http://www.twilert.com
Twime	http://www.twimemachine.com
Twint	https://github.com/haccer/twint
Twimap	https://twimap.com
Twipho	http://www.twipho.net
TwiSSR	http://www.twissr.com
Twitonomy	http://www.twitonomy.com
TwitRSS	https://twitrss.me
Twitter Account Details	http://www.twitteraccountsdetails.com
Twitter Advanced Search	https://twitter.com/search-advanced?lang=en
Twitter Audit	https://www.twitteraudit.com
Twitter BFTD	https://github.com/misterch0c/twitterBFTD
Twitter Chat Schedule	http://tweetreports.com/twitter-chat-schedule
Twitter Counter	http://twittercounter.com
Twitterfall	http://twitterfall.com
Twitter List Copy	http://projects.noahliebman.net/listcopy/index.php
Twitter Search	http://search.twitter.com
Twitter Search Tools	https://inteltechniques.com/menu.html
Twlets	http://www.twlets.com
Twopcharts	http://twopcharts.com
twoogel	http://twoogel.com
twXplorer	https://twxplorer.knightlab.com
TWUBS Twitter Chat	http://twubs.com/twitter-chats

unfollowgram	https://unfollowgram.com
Video Downloader for Twitter	http://www.downloadtwittervideo.com
Warble	https://warble.co

Social Media Tools: Facebook

Tool	Link
Agora Pulse	http://barometer.agorapulse.com
Aware Online Facebook Graph Search	https://www.aware-online.com/tips-voor-osint/facebook-graph-search/
Bulk Facebook ID Finder	http://seotoolstation.com/bulk-facebook-id-finder
Commun.it	http://commun.it
Custom Facebook Tools	https://inteltechniques.com/osint/facebook.html
Deturl.com Video Download	http://deturl.com/www.youtube.com/watch?v=uqnqLrakxY8
DownFacebook	http://www.downfacebook.com
Dredown	http://www.dredown.com
Expand All Facebook Comments	http://com.hemiola.com/2015/08/29/expand-all
ExtractFace	http://le-tools.com/ExtractFace.html#download
Facebook Like Checker	http://www.fblikecheck.com
Facebook Livemap	https://www.facebook.com/livemap
Facebook People Search	https://www.facebook.com/people-search.php
Facebook Search	https://search.fb.com
Facebook Search Tool	http://netbootcamp.org/facebook.html
Facebook Search Tools	https://inteltechniques.com/osint/facebook.html
Facebook Video Downloader	http://fbdown.net
Fanpage Karma	http://www.fanpagekarma.com
FB DOWN	https://www.fbdown.net
FB Scan Tool	http://pitoolbox.com.au/facebook-tool

Fb-sleep-stats	https://github.com/sqren/fb-sleep-stats
Find my Facebook ID	http://findmyfbid.com
Graph Tips	http://graph.tips
LikeAlyzer	http://likealyzer.com
Lookup-ID.com	https://lookup-id.com
peoplefindThor	https://www.peoplefindthor.dk
SaveVideo	http://savevideo.me
SearchIsBack	https://searchisback.com
Signal	https://signal.fb.com
Socialider Facebook Search	https://www.socialider.com/fbsearch
Social Fixer for Facebook	https://chrome.google.com/webstore/detail/social-fixer-for-facebook/ifmhoabcaeehkljcfclfiieohkohdgbb?hl=en
Socialsearching	http://socialsearching.info/#/fb
Socmint Tools	http://socmint.tools
StalkFace	https://stalkface.com
stalkscan	https://stalkscan.com
Wallfux	https://www.wallflux.com
Who posted what?	https://whopostedwhat.com
Wolfram Alpha Facebook Report	http://www.wolframalpha.com/input/?i=facebook+report
YouTube Comment Scraper	http://ytcomments.klostermann.ca
Zesty Facebook Search	http://zesty.ca/facebook

Social Media Tools: Google+

Tool	Link
CircleCount	http://www.circlecount.com
Google Plus Search	http://googleplussearch.chromefans.org
Lakako	https://www.lakako.com/google-plus
PlusFeed	http://plusfeed.frosas.net

Social Media Tools: Instagram

Tool	Link
Blocked and Banned Instagram Hashtag Search	http://thedatapack.com/tools/blocked-hashtag-search
Chrome IG Story	https://chrome.google.com/webstore/detail/chrome-ig-story/bojgejgifofondahckoaahkilneffhmf
Commun.it	https://commun.it
Custom Instagram Search Tools	https://inteltechniques.com/osint/instagram.html
DownloadGram	https://downloadgram.com
Find Instagram User ID	https://codeofaninja.com/tools/find-instagram-user-id
gramrix	https://gramrix.com
Hashtagify	http://hashtagify.me
Helper Tools for Instagram	https://chrome.google.com/webstore/detail/helper-tools-for-instagra/hcdbfckhdcpepllecbkaaojfgipnpbpb
Iconosquare	http://iconosquare.com
ImgToon	https://imgtoon.com
Ink361	http://ink361.com
Instagram User ID Finder	https://www.otzberg.net/iguserid/index.php
Instagram Search Tool	http://netbootcamp.org/instagram.html
Instagram User ID	http://www.ershad7.com/InstagramUserID
InstaLooter	https://github.com/althonos/InstaLooter
INSTATAGZ	http://instatagz.com
Instidy	http://instidy.com
Keyhole	http://keyhole.co
Lakako	https://www.lakako.com
Mininsta	http://mininsta.net
mulpix	https://mulpix.com

Mundimago Search People	http://www.mundimago.com/profile/search
Picbear	http://picbear.com
Picodash	https://www.picodash.com
Pictame	http://www.pictame.com
SnapMap	https://snapmap.knightlab.com
Social Rank	https://www.socialrank.com
Someture	http://someture.com
tailwind	https://www.tailwindapp.com
Tofo.me	https://tofo.me
Vibbi Instagram Web Viewer	https://vibbi.com/viewer
Webstagram	https://web.stagram.com/search
Websta	http://websta.me
Worldcam	http://worldc.am
Yooying	https://www.yooying.com

Social Media Tools: Pinterest

Tool	Link
Pingroupie	http://pingroupie.com
Pinterest Guest	https://addons.mozilla.org/en-US/firefox/addon/pinterest-guest
tailwind	https://www.tailwindapp.com

Social Media Tools: Reddit

Tool	Link
Ceddit	https://ceddit.com/r/all
Imgur	http://imgur.com
Karma Decay	http://karmadecay.com
Metareddit	http://metareddit.com
Mostly Harmless	http://kerrick.github.io/Mostly-Harmless/#features
Reddit All Comments Viewer Secure	https://chrome.google.com/webstore/detail/reddit-all-comments-viewe/hgpgeobpjpchpmkecjppgcnekmbibgbi?hl=en-GB
Reddit Archive	http://www.redditarchive.com
Reddit List	http://redditlist.com
Reddit Investigator	http://www.redditinvestigator.com
Reddit Metrics	http://redditmetrics.com
Reddit Suite	https://chrome.google.com/webstore/detail/reddit-enhancement-suite/kbmfpngjjgdllneeigpgjifpgocmfgmb
Reddit User Analyser	https://atomiks.github.io/reddit-user-analyser
Reddit Watch	https://redditwatch.com
Redective	http://redective.com
Reditr	http://reditr.com
Reeddit	https://reedditapp.com
ReSavr	https://www.resavr.com
Savvit.io	http://savvit.io
SnoopSnoo	http://snoopsnoo.com
Subreddits	http://subreddits.org

TopIAmA	https://www.topiama.com
uforio	http://uforio.com
Un-Delete Reddit Comments	https://chrome.google.com/webstore/detail/un-delete-reddit-comments/goelkfmlebeihlnanaindammeonplnhi

Social Media Tools: VKontakte

Tool	Link
Дезертир	http://vk.com/app3046467
Barkov.net	http://vk.barkov.net
Find Face	http://findface.ru
Report Tree	http://dcpu.ru/vk_repost_tree.php
Social Stats	http://socialstats.ru
SnRadar	http://snradar.azurewebsites.net
Spotlight	http://spotlight.svezet.ru
Target Hunter	https://targethunter.net
Target Log	http://targetolog.com
VK5	http://vk5.city4me.com
VK Community Search	http://vk.com/communities
VK Parser	http://vkparser.ru
VK People Search	http://vk.com/people
VK to RSS Appspot	http://vk-to-rss.appspot.com
vMetaDate	https://gist.github.com/cryptolok/8a023875b47e20bc5e64ba8e27294261

Social Media Tools: Tumblr

Tool	Link
Searchlr	http://searchlr.net
Tumblr Originals	http://studiomoh.com/fun/tumblr_originals
Tumblr Search	http://www.tumblr.com/search

Social Media Tools: LinkedIn

Tool	Link
Custom LinkedIn Search by Country	https://inteltechniques.com/osint/linkedin.country.html
Dux-Soup	http://www.dux-soup.com
Find Anyone's Email	https://chrome.google.com/webstore/detail/find-anyones-email-contac/jjdemeiffadmmjhkbbpglgnlgeafomjo
FTL	https://chrome.google.com/webstore/detail/ftl/lkpekgkhmldknbcgjicjkomphkhhdkjj?hl=en-GB
Linkedin2username	https://github.com/initstring/linkedin2username
LinkedIn Guest Browser	https://addons.mozilla.org/en-US/firefox/addon/linkedin-guest-browser
raven	https://github.com/0x09AL/raven
ScrapedIn	https://github.com/dchrastil/ScrapedIn
socilab	http://socilab.com
the-endorser	https://github.com/eth0izzle/the-endorser

Social Media Tools: Snapchat

Tool	Link
FindMySnap	http://findmysnap.com
snapdex	https://www.snapdex.com
Snap Map	https://map.snapchat.com
Snap VIP	https://snapvip.io
Somechater	http://somechater.com

Social Media Tools: WhatsApp

Tool	Link
WhatsAllApp	https://github.com/LoranKloeze/WhatsAllApp
WhatsApp Fake Chat	http://www.fakewhats.com/generator
whatsfoto	https://github.com/zoutepopcorn/whatsfoto

Social Media Tools: Skype

Tool	Link
CyberHub Resolver	http://cyber-hub.net/resolver.php
Web Resolver	https://webresolver.nl

Social Media Tools: Telegram

Tool	Link
Save-telegram-chat-history	https://github.com/pigpagnet/save-telegram-chat-history
Telegram Channels Catalog	https://tchannels.me
Telegram Search	http://tsear.ch

Other Instant Messaging and Chat Tools

Tool	Link
Botbot.me	https://botbot.me
icq	https://icq.com/people
IRC Search	http://irc.netsplit.de/channels/search.php
ircsnapshot	https://github.com/bwall/ircsnapshot
mibbit	http://mibbit.com

Dating Apps

Tool	Link
Dating Apps and Sites for Investigators by Emmanuelle Welch	https://start.me/p/VRxaj5/dating-apps-and-sites-for-investigators

Blogs, Forums, Discussion Boards, and Q&A Sites

Blog Search

Tool	Link
Bloghunt	https://bloghunt.me
BlogSeacrhEngine	http://www.blogsearchengine.org
NetworkedBlogs	http://www.networkedblogs.com
Notey	https://www.notey.com
Twingly	http://www.twingly.com
Webhose.io	https://webhose.io

Forums and Discussion Boards Search

Tool	Link
BoardReader	http://boardreader.com
Delphi Forums	http://www.delphiforums.com
Facebook Groups	https://www.facebook.com
Foren User	http://www.forenuser.de
Google Groups	https://groups.google.com
Hoood.de	http://www.hoood.de
Linkedin Groups	http://www.linkedin.com
Ning	http://www.ning.com
Xing Groups	https://www.xing.com/communities
Webhose.io	https://webhose.io
Yahoo Groups	https://groups.yahoo.com

Q&A Sites

Tool	Link
Answers.com	http://www.answers.com
Ask	http://www.ask.com
Ask.fm	https://ask.fm
eHow	http://www.ehow.com
gutefrage	https://www.gutefrage.net
Quora	http://www.quora.com
StackExchange	http://stackexchange.com
Yahoo Answers	http://answers.yahoo.com

People Investigations

Main People Search Tools and Engines

Tool	Link
411 (US)	http://www.411.com
Addresses (US)	http://www.addresses.com
Alumni.net	http://www.alumni.net
AnyWho (US)	https://www.anywho.com/whitepages
Classmates	http://www.classmates.com
CrunchBase	http://www.crunchbase.com
Custom Person Search Tool	https://inteltechniques.com/osint/person.html
Data.com Connect	https://connect.data.com
dataScrape	https://github.com/khayes-r7/dataScrape
Discoverly	https://chrome.google.com/webstore/detail/discoverly-for-gmail-link/dijhcpbkalfgkcebgoncjmfpbamihgaf \|\| https://discover.ly
Gaddr	https://gaddr.me
facesearch	http://facesaerch.com
FTL	https://chrome.google.com/webstore/detail/fullcontact-for-gmail/cnaibnehbbinoohhjafknihmlopdhhip
GPSies	https://www.gpsies.com/trackList.do
Gravatar	http://en.gravatar.com
Hey Press (Search for Journalists)	https://www.hey.press
HowManyOfMe	http://howmanyofme.com/search
HIRETUAL	https://chrome.google.com/webstore/detail/hiretual-10x-faster-talen/jeablngoapekimaeoeclgcefdcpjhjcg

Intelius (US)	https://www.intelius.com
Itools	http://itools.com/search/people-search \|\| http://itools.com/tool/wink-people-search
John Doe (US)	https://johndoe.com
Keybase	https://keybase.io
LittleSis	https://littlesis.org
LookUp	http://www.lookup.com
LookUpUK	http://www.lookupuk.com
ManyContacts Mail Check	https://www.manycontacts.com/en/mail-check
MarketVisual	http://www.marketvisual.com
NameScan	https://namescan.io
Neighbor Report	https://neighbor.report
Nextdoor	https://nextdoor.com
Nuwber	https://nuwber.com
Nuwber	https://nuwber.co.no
peekyou	https://www.peekyou.com
Peoplefinders (US)	https://www.peoplefinders.com
People Looker (US)	https://www.peoplelooker.com
People Search	http://netbootcamp.org/peoplesearch.html
People Search (Australia)	http://www.peoplesearch.com.au
PeopleSmart (US)	https://www.peoplesmart.com
PersonLookup.com	http://www.personlookup.com
FastPeopleSearch (US)	https://www.fastpeoplesearch.com
PimEye	https://pimeyes.com/en
pipl	https://pipl.com
Profile Engine	http://profileengine.com
Profilr	https://www.profilr.social/search/jsmith
Recruit'em	http://recruitin.net
Research.com (US)	https://www.research.com
Reverse Genie	http://www.reversegenie.com
Skimleads	http://skimleads.com
Skipease (US)	http://www.skipease.com
Smugmug	https://www.smugmug.com/search

Snitch.name	http://www.snitch.name
Snoop Station (US)	http://snoopstation.com
Social catfish	https://socialcatfish.com
Speedy Hunt (US)	https://speedyhunt.com
Spokeo	http://www.spokeo.com
Spytox (US)	https://www.spytox.com
Strava	https://labs.strava.com/heatmap
TalentBin	https://www.talentbin.com
TruePeopleSearch (US)	https://www.truepeoplesearch.com
ufind.me	http://ufind.name
UserSearch	https://usersearch.org
USSEARCH (US)	https://www.ussearch.com
WebMii	http://www.webmii.com
Yasni	http://www.yasni.com
Zoominfo	http://www.zoominfo.com

Address & Contact Information Search

Tool	Link
118172	https://www.118712.fr
192 (UK)	http://www.192.com
411 (US)	http://www.411.com
Addresses (US)	http://www.addresses.com
Address Search (US)	http://www.addresssearch.com
AnyWho (US)	https://www.anywho.com/yellow-pages
Australia Lookup	http://www.australialookup.com
BeenVerified (US)	https://www.beenverified.com
Canada411(Canada)	http://www.canada411.ca
Data 24-7	https://www.data24-7.com
Find People Search (US)	http://www.findpeoplesearch.com
HomeMetry	https://homemetry.com
Infobel	http://www.infobel.com/en/world
John Doe (US)	https://johndoe.com
PeopleSmart (US)	https://www.peoplesmart.com
FastPeopleSearch (US)	https://www.fastpeoplesearch.com
SearchBug (US)	http://www.searchbug.com
Spytox (US)	https://www.spytox.com
That'sThem	https://thatsthem.com
TruePeopleSearch (US)	https://www.truepeoplesearch.com
USSearch (US)	https://www.ussearch.com
Verispy (US)	https://www.verispy.com/people-search
White Pages	http://www.whitepages.com
whowhere	http://www.whowhere.com

Zabasearch	http://www.zabasearch.com

Public Records

Tool	Link
Advanced Background Checks (US)	https://www.advancedbackgroundchecks.com
Australia Public Records	http://australiapublicrecord.com
Birth Database	http://www.birthdatabase.com
Black Book Online (US)	https://www.blackbookonline.info
BRBPub.com	http://www.brbpub.com
Crime Reports (US)	https://www.crimereports.com
Criminal Searches (US)	https://www.criminalsearches.com
Cubib (US)	http://cubib.com
DOBSEARCH	https://www.dobsearch.com
Family Watchdog (US)	https://www.familywatchdog.us
Federal Bureau of Prisons - Inmate Locator (US)	http://www.bop.gov/inmateloc
Felon Spy (US)	http://www.felonspy.com
Find A Grave (US)	https://www.findagrave.com
Find People Search (US)	https://findpeoplesearch.com
Fold3 (US Military Records)	http://www.fold3.com
Free Public Records Directory (US)	http://publicrecords.onlinesearches.com
golookup (US)	https://golookup.com
GOVDATACA (Canada)	https://govdataca.com
Grave Info (US)	http://www.graveinfo.com
Inmate Locator (US)	http://www.theinmatelocator.com
Inmate Locator (US)	https://www.bop.gov/inmateloc
Intelius (US)	https://www.intelius.com
Interment (Cemetery Records)	http://www.interment.net/data/search.htm

Instant Checkmate	https://www.instantcheckmate.com
Investigative Dashboard Search	https://data.occrp.org
Legacy.com (US)	http://www.legacy.com
Melissa (US)	http://melissadata.com
NETR ONLINE (US)	https://publicrecords.netronline.com
NSOPW (US)	https://www.nsopw.gov/en/Search/Verification
Orbituaries Australia	http://oa.anu.edu.au
Peoplefinder (US)	https://www.peoplefinders.com
Political MoneyLine (US)	http://www.politicalmoneyline.com
Public Info Directory (US)	https://publicrecords.directory
Public Records (Australia)	https://www.publicrecords.com.au
Radaris	http://radaris.com
RecordsPedia	http://recordspedia.com
Reunion (US)	http://www.reunion.com
SCRA Website (US)	https://scra.dmdc.osd.mil/scra/#/home
Sorted by Birth Date	http://sortedbybirthdate.com
Speedy Hunt	https://speedyhunt.com
SSN Validator	https://www.ssnvalidator.com
UniCourt	https://unicourt.com
USSEARCH (US)	https://www.ussearch.com
Voter Registration Records (US)	https://voterrecords.com

Ancestry Research

Tool	Link
Ancestor Hunt	http://ancestorhunt.com
Ancestry	http://www.ancestry.com
Family Search	https://familysearch.org
FamilyTreeNow	http://www.familytreenow.com
Find my past	https://search.findmypast.com/search-world-records
Forebears	http://forebears.io
FreeBMD	https://www.freebmd.org.uk
Genealogy	https://www.genealogy.com
Genealogy Bank	http://www.genealogybank.com
Genealogy in Time	http://www.genealogyintime.com
Genealogy Links	http://www.genealogylinks.net
Locate Family	https://www.locatefamily.com
Mocavo	https://www.findmypast.com/mocavo-info
The National Archives UK	http://www.nationalarchives.gov.uk
Rootsweb	http://home.rootsweb.ancestry.com
Search for Ancestors	http://www.searchforancestors.com
Sorted By Name	http://sortedbyname.com

Phone Search

Tool	Link
411 (US)	https://www.411.com/reverse-phone
Abc telefonos	http://www.abctelefonos.com
Addresses (US)	http://www.addresses.com
AnyWho (US)	https://www.anywho.com/reverse-lookup
Australia Lookup	http://www.australialookup.com
Blacklist Checker	https://imei24.com/blacklist_check
Bmobile.in	https://bmobile.in
British Phone Book	http://www.britishphonebook.com
BT Phone Book	https://www.thephonebook.bt.com
CallerID Service	https://secure.calleridservice.com
CallerID Test	https://www.calleridtest.com
CallerSmart	https://www.callersmart.com
Carrier Lookup	https://www.carrierlookup.com
Carrier Lookup Service	http://freecarrierlookup.com
CellRevealer	https://cellrevealer.com
CountryCode	https://countrycode.org
Custom Telephone Search	https://inteltechniques.com/OSINT/telephone.html
FastPeopleSearch (US)	https://www.fastpeoplesearch.com
Fone Finder	http://www.fonefinder.net
Free Carrier Lookup (US)	https://freecarrierlookup.com
golookup	https://golookup.com
IMEI24	https://imei24.com
International Numbering Plans	https://www.numberingplans.com

International White and Yellow Pages	http://www.wayp.com
Ivycall	http://www.ivycall.com
John Doe (US)	https://johndoe.com
Keecall (US)	http://www.keecall.us
Leaked Source	https://leakedsource.ru
MailTester	http://mailtester.com/testmail.php
MrNumber (US)	http://mrnumber.com/1-888-742-0000
nextcaller	https://nextcaller.com
Number Guru	https://www.numberguru.com
NumberVille	https://numberville.com
numberway	https://www.numberway.com
numpi	https://numpi.com
NumSpy	https://bhattsameer.github.io/numspy
peoplebyname	http://www.peoplebyname.com
People Call	https://www.peoplecall.com
Peoplefinders (US)	https://www.peoplefinders.com
People Looker (US)	https://www.peoplelooker.com
PeopleSmart (US)	https://www.peoplesmart.com
Phone Book of the World	http://pbof.com
phoneowner	https://phoneowner.com
PhoneSearchFree (US)	https://www.phonesearchfree.com
Phone Tools	https://inteltechniques.com/osint/telephone.html
PhoneValidator	https://www.phonevalidator.com
Open Cnam	https://www.opencnam.com
Reverse Genie (US)	http://www.reversegenie.com/phone.php
SearchYellowDirectory	http://www.searchyellowdirectory.com
Snusbase	https://snusbase.com
Social catfish: Reverse Phone Lookup	https://socialcatfish.com/reverse-phone-lookup
Speedy Hunt	https://speedyhunt.com
Spy Dialer (US)	https://www.spydialer.com
Spy on Caller	http://spyoncaller.net

Spytox (US)	https://www.spytox.com
Sync.me	https://sync.me
Telefonbuch	http://www.telefonbuch.com
TextMagic Free Carrier Lookup	https://www.textmagic.com/free-tools/carrier-lookup
That's Them: Reverse Phone Lookup	https://thatsthem.com/reverse-phone-lookup
Truecaller	https://www.truecaller.com
TruePeopleSearch (US)	https://www.truepeoplesearch.com
Twilio	https://www.twilio.com/lookup
USPhoneBook	https://www.usphonebook.com
USSEARCH (US)	https://www.ussearch.com
Whocalld	https://whocalld.com
Vigilante	https://www.vigilante.pw
Zonzoo	http://zonzoo.nl

E-mail Search / E-mail Check

Tool	Link
411 (US)	http://www.411.com
Ashley Madison Hack	https://ashley.cynic.al
BotScout	https://botscout.com/search.htm
BreachAlarm	https://breachalarm.com
BriteVerify Email Verification	http://www.briteverify.co.uk
Cellular Email Assumptions	https://inteltechniques.com/osint/cellperm.html
Clearbit Connect	https://chrome.google.com/webstore/detail/clearbit-connect-supercha/pmnhcgfcafcnkbengdcanjablaabjplo?hl=en
Custom Email Search Tools	https://inteltechniques.com/osint/menu.email.html
DomainBigData	https://domainbigdata.com
Email4Corporations	https://sites.google.com/site/emails4corporations/home
Email Address Validator	http://www.email-validator.net
Email Assumptions	https://inteltechniques.com/osint/email.html
Email Checker	https://email-checker.net
EmailDrop	https://chrome.google.com/webstore/detail/emaildrop-extract-emails/peilgijmhiocdmdeglhiljipigamfbjh
Email Extractor	https://chrome.google.com/webstore/detail/email-extractor/jdianbbpnakhcmfkcckaboohfgnngfcc?hl=en
Email Extractor	http://emailx.discoveryvip.com

Email Extractor Lite	http://eel.surf7.net.my
Email Format	http://email-format.com
Email Generator	http://emailgenerator.io
Email Guesser	http://www.guesser.email
Email Header Analyzer	https://mxtoolbox.com/EmailHeaders.aspx
EmailHippo	https://tools.verifyemailaddress.io
Email Hunter	https://hunter.io
Email Location	http://www.melissadata.com/lookups/email-location.asp
emailmatcher	https://emailmatcher.com
Email Permutator+	http://metricsparrow.com/toolkit/email-permutator
Emails4corporations	https://sites.google.com/site/emails4corporations/home
EmailSearch.org	http://www.email-search.org/search-emails
Email Validator	https://www.email-validator.net
FindThatLead	https://findthatlead.com
Free Email Verifier	http://verify-email.org
Gawker Hack Email Check	https://labs.duo.com/gawker
Github-osint	https://github.com/hackstep/github-osint
Googligan Checker	https://gooligan.checkpoint.com
Gotcha	https://gotcha.pw
Gravatar Email Check	http://en.gravatar.com/site/check
Hacked Emails	https://hacked-emails.com
Have I Been Pwned	https://haveibeenpwned.com
Have I Been Sold	https://haveibeensold.app
headreach	https://headreach.com
HPI Identity Leak Checker	https://sec.hpi.uni-potsdam.de/ilc/search;jsessionid=A94B3A03C67B00F3B0FADB4A8C08E6FA

Hunter	https://hunter.io
Infoga	https://github.com/m4ll0k/infoga
Leaked Source	https://leakedsource.ru
Mail Jagger	https://mailjagger.ga
MailTester	http://mailtester.com/testmail.php
Many Contacts Email Check	https://www.manycontacts.com/en/mail-check
Melissa (US)	http://www.melissadata.com/lookups/emails.asp
OSINTTOOLKIT Email	https://osinttoolkit.github.io/EmailUsername
Peepmail	http://www.samy.pl/peepmail
People Looker (US)	https://www.peoplelooker.com
PeopleSmart (US)	https://www.peoplesmart.com
Pipl	https://pipl.com
Polities	https://www.politie.nl/themas/controleer-of-mijn-inloggegevens-zijn-gestolen.html
Prospect Linked	https://prospectlinked.com
Public E-mail Records	http://publicemailrecords.com
Read Notify	http://www.readnotify.com
Reverse Genie E-mail	http://www.reversegenie.com/email.php
sellhack	https://sellhack.com
Snusbase	https://snusbase.com
Speedy Hunt	https://speedyhunt.com
SPYDialer	https://www.spydialer.com
Spytox (US)	https://www.spytox.com
TCIPUTILS.com Email Test	http://www.tcpiputils.com/email-test
That'sThem	https://thatsthem.com/reverse-email-lookup
Toofr	https://www.toofr.com
USSEARCH (US)	https://www.ussearch.com

Validate Email Address	https://validateemailaddress.org
Verifalia	http://verifalia.com/validate-email
Verify Email	https://verify-email.org
Verify Email Account	https://es.infobyip.com/verifyemailaccount.php
Verify Email Address	https://tools.verifyemailaddress.io
VoilaNorbert	https://www.voilanorbert.com

Username Check

Tool	Link
Check User Names	http://www.checkusernames.com
Custom User Name Search	https://inteltechniques.com/osint/username.html
Gaddr	https://gaddr.me
Knowem	http://www.Knowem.com
Leaked Source	https://leakedsource.ru
Lullar	http://com.lullar.com
Name Checkr	http://www.namecheckr.com
Name Chk	http://www.namechk.com
Namech_k.sh	https://github.com/HA71/Namechk
Name Vine	https://namevine.com
OSINTTOOLKIT Username	https://osinttoolkit.github.io/EmailUsername
peekyou	https://www.peekyou.com
pipl	https://pipl.com
Snitch.name	http://snitch.name
Snusbase	https://snusbase.com
Speedy Hunt (US)	https://speedyhunt.com
Spokeo	https://www.spokeo.com
Usercard	http://usercard.org
User Search	http://www.usersearch.org
User Sherlock	http://usersherlock.com
Vigilante	https://www.vigilante.pw
WhatsMyName	https://github.com/WebBreacher/WhatsMyName

CV and Resume Search

Tool	Link
Custom Hidden Resume Search	https://inteltechniques.com/osint/hidden.resumes.html
CVGadget	http://www.cvgadget.com
Indeed	https://www.indeed.com
LeadFerret	https://leadferret.com/search
Linkedin	https://www.linkedin.com
MarketVisual	http://www.marketvisual.com
Recruit'em	https://recruitin.net
Visualize.me	http://vizualize.me
XING	https://www.xing.com

Expert Search

Tool	Link
Academia	http://academia.edu
CanLaw	http://www.canlaw.com
expertfile	https://expertfile.com
ExpertiseFinder	http://www.expertisefinder.com
ExpertGuide	http://www.expertguide.com.au
ExpertPages	http://expertpages.com
Experts.com	http://www.experts.com
HARO	http://www.helpareporter.com
GlobalExperts	http://www.theglobalexperts.org
Idealist	http://www.idealist.org
Innocentive	http://www.innocentive.com
Internet Experts	http://www.internetexperts.info
Library of Congress: Ask a Librarian	http://www.loc.gov/rr/askalib
Maven	http://www.maven.co
MuckRack	http://muckrack.com
National Speakers Association	http://www.nsaspeaker.org
Newswise	http://www.newswise.com
Patent Attorneys/Agent Search	https://oedci.uspto.gov/OEDCI
PRNewswire	https://prnmedia.prnewswire.com
ProfNet	http://www.prnewswire.com/profnet
ReseacherID	http://www.researcherid.com
ScholarUniverse	http://www.scholaruniverse.com
SheSource	http://www.womensmediacenter.com/shesource
speakezee	https://www.speakezee.org

Sources	http://www.sources.com
TRExpertWitness	https://www.trexpertwitness.com
Zintro	https://www.zintro.com

Salary Search

Tool	Link
Adecco USA	https://www.adeccousa.com/resources/salary-calculator
AFL-CIO Executive Paywatch	https://aflcio.org/paywatch
CareerBliss	https://www.careerbliss.com/salary
Career Boutique	https://www.careerboutique.com/salary
Career Builder	https://www.careerbuilder.com
Career One Stop	https://www.careeronestop.org/Toolkit/Wages/find-salary.aspx
Glassdoor Salaries	https://www.glassdoor.com/Salaries/index.htm
Equilar	http://www.equilar.com
Indeed Salaries	https://www.indeed.com/salaries
Job Search Intelligence	https://www.jobsearchintelligence.com/etc/jobseekers/salary-calculator.php
Live Career	https://www.livecareer.com/salary
Monster Salary	https://www.monster.com/salary
Payscale	https://www.payscale.com/research/US/Country=United_States/Salary
Paysa	https://www.paysa.com/salaries-list/company
Pay Wizard	https://paywizard.org/main/salary/calculator#
RAPS.org	https://www.raps.org/careers/salary-calculator
Salary.com	https://www.salary.com
Salary Expert	https://www.salaryexpert.com

Simply Hired Salary Estimator	https://www.simplyhired.com/salaries
Salary List	http://www.salarylist.com
United States Department of Labor	https://www.bls.gov/ooh
US Experteer	https://us.experteer.com/salary_calculator
Wall Street Oasis Salary Search	https://www.wallstreetoasis.com/wso-company-database/salary

Creating a Sock Puppet

Tool	Link
Behind the Name	https://www.behindthename.com/random
Fake Identity Generator	http://backgroundchecks.org/justdeleteme/fake-identity-generator
Fake Name Generator	https://www.fakenamegenerator.com
Fake Person Generator	https://www.fakepersongenerator.com
Data Fake Generator	http://www.datafakegenerator.com/generador.php
List of Random Names	http://listofrandomnames.com
Name Fake	https://en.namefake.com
Random Name Generator	http://random-name-generator.info/random/?n=10&g=1&st
Sudo App	https://sudoapp.com

Company Research

Main Company Search Tools and Engines

Tool	Link
AIHIT	https://www.aihitdata.com
AllStocksLinks	http://www.allstocks.com/links
AngelList	https://angel.co
Annual Reports	http://www.annualreports.com
Big Red Directory	https://www.bigreddirectory.com
bikudo	https://www.bikudo.com
Bizeurope	http://www.bizeurope.com
Biznar	https://biznar.com
Bizstats	http://www.bizstats.co.uk
Bizstats	http://www.bizstats.com
Bloomberg	http://www.bloomberg.com/research/company/overview/overview.asp
brandchecker	https://brandchecker.com
Business Source	https://www.ebscohost.com/academic/business-source-complete
Bureau Van Dijk	http://www.bvdinfo.com
Buzzfile	http://www.buzzfile.com
Canadian Business Research	https://www.canada.ca/en/services/business/research.html
Canadian Business Resource	http://www.cbr.ca
Cedar Rose	https://www.cedar-rose.com
Checktrade	https://www.checkatrade.com

Comparably	https://www.comparably.com
CompeteShark	http://competeshark.com
Corporate Information	http://www.corporateinformation.com
Corporation Wiki	https://www.corporationwiki.com
CorpWatch	http://www.corpwatch.org
Crunchbase	https://www.crunchbase.com
Data.com Connect	https://connect.data.com
Dun & Bradstreet	https://www.dnb.com
EDGAR Online	http://www.edgar-online.com
Engineering 360	https://www.globalspec.com
Euromonitor	http://www.euromonitor.com
Europages	http://www.europages.co.uk
Ezilon	http://www.ezilon.com
Factiva	https://global.factiva.com
Forbes Global 2000	http://www.forbes.com/global2000/
Fortune Global 500	http://fortune.com/global500
Foursquare	https://foursquare.com
Glassdoor	https://www.glassdoor.com
globalEdge	http://globaledge.msu.edu
Google Finance	https://www.google.com
GuideStar	http://www.guidestar.org
Hoovers	http://www.hoovers.com
HotFrog	https://www.hotfrog.com
Inc. 5000	http://www.inc.com/inc5000
infobel	https://www.infobel.com
Infocif (Spain)	http://www.infocif.es
Info clipper	http://www.info-clipper.com
InstantLogoSearch	http://instantlogosearch.com
iSpionage	https://www.ispionage.com
Investigative Dashboard Search	https://data.occrp.org
Kompass	https://www.kompass.com
Kyckr	https://portal.kyckr.co.uk

Linkedin	https://www.linkedin.com
LittleSis	https://littlesis.org
Mapped in Israel	https://mappedinisrael.com
Manta	https://www.manta.com
MarketLine	http://marketline.com
MarketVisual	http://www.marketvisual.com
Mergent Intellect	http://www.mergentintellect.com
Mergent Online	http://www.mergentonline.com/login.php
Mint Global	https://mintglobal.bvdinfo.com
Morningstar Research	http://library.morningstar.com
Notablist	https://www.notablist.com
orbis directory	https://orbisdirectory.bvdinfo.com
opencorporates	https://opencorporates.com
Owler	https://www.owler.com
Plunkett Research	http://www.plunkettresearchonline.com
The Public Register	http://www.annualreportservice.com
The Public Register	http://www.prars.com/search/alpha/A
Quandl	https://www.quandl.com
Report Linker	https://www.reportlinker.com
Ripoff Report	http://www.ripoffreport.com
Sqoop	https://sqoop.com
Skimleads	http://skimleads.com
SpyFu	https://www.spyfu.com
Startupexplore	https://startupxplore.com/en/startups
ThomasNet	https://www.thomasnet.com
Usercard	http://usercard.org
Vault	http://www.vault.com
Xing	http://www.xing.com
Yahoo Finance	https://finance.yahoo.com
Zauba Corp	https://www.zaubacorp.com
Zoominfo	https://www.zoominfo.com/companies-search

Company Research (EU)

Tool	Link
Bizeurope	http://www.bizeurope.com
Central and Eastern European Business Directory	http://www.ceebd.co.uk/ceebd
Company Registration Round the World	http://www.commercial-register.sg.ch/home/worldwide.html
Company Research Resources by Country	http://www.rba.co.uk/sources/registers.htm
De Telefoongids (Netherlands)	https://www.detelefoongids.nl
Europages	http://www.europages.co.uk
European Business Register	http://www.ebr.org
Ezilon	http://www.ezilon.com
Foursquare	https://foursquare.com
Global Business Register	http://www.globalbusinessregister.com
Knowledge guide to international company registration	http://www.icaew.com/en/library/subject-gateways/business-management/company-administration/knowledge-guide-international-company-registration
Kompass	https://www.kompass.com
Kyckr	https://portal.kyckr.co.uk
Libreborme	https://libreborme.net
National Company Registers	https://en.wikipedia.org/wiki/List_of_company_registers
opencorporates	https://opencorporates.com
SEMrush	https://www.semrush.com
Skimleads	http://skimleads.com
Startupexplore	https://startupxplore.com/en/startups

Company Research (UK)

Tool	Link
Big Red Directory	https://www.bigreddirectory.com
BizDB	http://www.bizdb.co.uk
Bizstats	http://www.bizstats.co.uk
Central and Eastern European Business Directory	http://www.ceebd.co.uk/ceebd
Claims Management Regulation – Authorised Business Register	https://www.claimsregulation.gov.uk/search.aspx
Companies in the UK	https://www.companiesintheuk.co.uk
Company Registration Round the World	http://www.commercial-register.sg.ch/home/worldwide.html
Company Research Resources by Country	http://www.rba.co.uk/sources/registers.htm
Cylex (UK)	https://www.cylex-uk.co.uk
ELTO (UK)	https://eld.elto.org.uk
Elucify (UK)	https://www.elucify.com

Employment Tribunal Decisions (UK)	https://www.gov.uk/employment-tribunal-decisions
Europages	http://www.europages.co.uk
European Business Register	http://www.ebr.org
Ezilon	http://www.ezilon.com
Fair Trades	http://www.fairtrades.co.uk
Financial Conduct Authority Search (UK)	https://www.fca.org.uk/search-results?search_term=clone%20firm%20details&start=1&sort_by=dmetaZ
Foursquare	https://foursquare.com
Food Hygiene Ratings (UK)	https://www.scoresonthedoors.org.uk//index.php
Global Business Register	http://www.globalbusinessregister.com
iSpionage	https://www.ispionage.com
Knowledge guide to international company registration	http://www.icaew.com/en/library/subject-gateways/business-management/company-administration/knowledge-guide-international-company-registration
Kompass	https://www.kompass.com
Kyckrs	https://portal.kyckr.co.uk
Local Heroes	https://www.localheroes.com
My Builder	https://www.mybuilder.com
National Company Registers	https://en.wikipedia.org/wiki/List_of_company_registers
NicEic	http://www.niceic.com
Opening Times (UK)	https://www.opening-times.co.uk
orbis directory	http://orbisdirectory.bvdinfo.com/version-20161014/OrbisDirectory/Companies

opencorporates	https://opencorporates.com
Overseas Company Registers	https://www.gov.uk/government/publications/overseas-registries/overseas-registries
Scoot	http://www.scoot.co.uk
SEMrush	https://www.semrush.com
Skimleads	http://skimleads.com
Stall Finder	https://www.stallfinder.com
Tradesmen Corner (UK)	https://www.tradesmencorner.co.uk
Trustatrader	https://www.trustatrader.com
Trust Mark (UK)	https://www.trustmark.org.uk
Trust Pilot (UK)	https://uk.trustpilot.com
UK Companies List	https://www.companieslist.co.uk
UK Data	http://ukdata.com
Yell	https://www.yell.com

Company Research (US)

Tool	Link
Better Business Bureau	http://www.bbb.org
Business Source	https://www.ebscohost.com/academic/business-source-complete
Company Registration Round the World	http://www.commercial-register.sg.ch/home/worldwide.html
Company Research Resources by Country	http://www.rba.co.uk/sources/registers.htm
Comparably	https://www.comparably.com
Corporation wiki	https://www.corporationwiki.com
EDGAR Online	http://www.edgar-online.com
Ezilon	http://www.ezilon.com
Foursquare	https://foursquare.com
Glassdoor	https://www.glassdoor.com
Global Business Register	http://www.globalbusinessregister.com
GuideStar	http://www.guidestar.org
Inc. 5000	http://www.inc.com/inc5000
iSpionage	https://www.ispionage.com
Knowledge guide to international company registration	http://www.icaew.com/en/library/subject-gateways/business-management/company-administration/knowledge-guide-international-company-registration
Kompass	https://www.kompass.com
Kyckr	https://portal.kyckr.co.uk
LinkSV	http://www.linksv.com
National Company Registers	https://en.wikipedia.org/wiki/List_of_company_registers

Manta	https://www.manta.com
MarketLine	http://marketline.com
Mergent Online	http://www.mergentonline.com
Morning Star	http://www.morningstar.com
orbis directory	https://orbisdirectory.bvdinfo.com
opencorporates	https://opencorporates.com
Owler	https://www.owler.com
PrivCo	https://www.privco.com
SEMrush	https://www.semrush.com
Skimleads	http://skimleads.com
Stall Finder	https://www.stallfinder.com
Startupexplore	https://startupxplore.com/en/startups
Vault	http://www.vault.com
Wall street Oasis	https://www.wallstreetoasis.com/wso-company-database

Company Research (Switzerland)

Tool	Link
Company Research Resources by Country	http://www.rba.co.uk/sources/registers.htm
Knowledge guide to international company registration	http://www.icaew.com/en/library/subject-gateways/business-management/company-administration/knowledge-guide-international-company-registration
Kompass	https://www.kompass.com
Kyckr	https://portal.kyckr.co.uk
National Company Registers	https://en.wikipedia.org/wiki/List_of_company_registers
orbis directory	http://orbisdirectory.bvdinfo.com/version-20161014/OrbisDirectory/Companies
SEMrush	https://www.semrush.com
Skimleads	http://skimleads.com

Company Research (Middle East)

Tool	Link
Bahrain	*http://www.big.bh/einvestor.web*
Dubai	*https://www.difc.ae/setting-up*
Ezilon	*http://www.ezilon.com*
Israel	*http://www.justice.gov.il/En/Pages/default.aspx*
Jordan	*http://ccd.gov.jo*
Kompass	*https://www.kompass.com*
Kyckr	*https://portal.kyckr.co.uk*
Mapped in Israel	*https://mappedinisrael.com*
National Company Registers	*https://en.wikipedia.org/wiki/List_of_company_registers*
SEMrush	*https://www.semrush.com*
Skimleads	*http://skimleads.com*

Company Research (Africa)

Tool	Link
BCE (Senegal)	http://creationdentreprise.sn/rechercher-une-societe
CCI (Burkina Faso)	http://www.cci.bf/?q=fr/entreprise
CCIMA (Cameroon)	http://www.ccima.cm
Cedar Rose	https://www.cedar-rose.com
CEPICI (Ivory Coast)	https://www.cepici.ci
CIPC	http://www.cipc.co.za/za
Clarified By	https://www.clarifiedby.com
CNRC (Algeria)	https://sidjilcom.cnrc.dz
Companies and Intellectual Property Commission (South Africa)	https://eservices.cipc.co.za
Company Research Resources by Country	http://www.rba.co.uk/sources/registers.htm
Directinfo.ma (Marocco)	https://www.directinfo.ma
Ezilon	http://www.ezilon.com
GUFE-RCA	http://gufe-rca.org
Kompass	https://www.kompass.com
Kyckr	https://portal.kyckr.co.uk
National Company Registers	https://en.wikipedia.org/wiki/List_of_company_registers
Nigeria Corporate Affairs Commission	http://new.cac.gov.ng
Registre de commerce de Tunisie	https://www.registre-commerce.tn
SEMrush	https://www.semrush.com
Skimleads	http://skimleads.com

South Africa	http://www.cipc.co.za/za

Company Research (China)

Tool	Link
China	https://www.cr.gov.hk
Ezilon	http://www.ezilon.com
Kompass	https://www.kompass.com
Kyckr	https://portal.kyckr.co.uk
National Company Registers	https://en.wikipedia.org/wiki/List_of_company_registers
SEMrush	https://www.semrush.com
Skimleads	http://skimleads.com

Business Registers (EU + EFTA)

Tool	Link
United Kingdom: Authorised Business Register	https://www.claimsregulation.gov.uk/search.aspx
United Kingdom: Companies House	https://www.gov.uk/government/organisations/companies-house
European Business Register	http://www.ebr.org
National Company Registers	https://en.wikipedia.org/wiki/List_of_company_registers
Austria	http://www.justiz.gv.at/firmenbuch
Belgium	http://www.eurodb.be
Bulgaria	http://www.brra.bg
Cyprus	http://www.mcit.gov.cy/mcit/drcor/drcor.nsf/index_en/index_en?opendocument
Czech Republic	https://www.mfcr.cz
Denmark	https://datacvr.virk.dk/data
Estonia	https://ariregister.rik.ee/mobile/mobile/select
Finland	https://www.prh.fi/en/index.html
France	https://www.infogreffe.fr
France	https://www.inpi.fr
Germany	https://www.unternehmensregister.de/ureg/?submitaction=language&language=en
Greece	http://www.acci.gr/acci/shared/index.jsp?context=101
Hungary	https://www.e-cegjegyzek.hu
Iceland	https://www.rsk.is/english/individuals
Ireland	https://www.statice.is
Italy	http://www.infocamere.it/en/home
Latvia	https://www.ur.gov.lv/lv

Lithuania	http://www.registrucentras.lt/en
Luxembourg	https://www.rcsl.lu/mjrcs/jsp/IndexActionNotSecured.action?time=1525227992196&loop=2
Malta	https://registry.mfsa.com.mt/ROC
Netherlands	https://www.kvk.nl
Poland	https://www.ms.gov.pl/en/about-the-ministry-of-justice
Portugal	http://www.irn.mj.pt/IRN/sections/inicio
Romania	https://e-justice.europa.eu/content_business_registers-104-en.do
Slovakia	http://www.orsr.sk/default.asp?lan=en
Slovenia	https://www.ajpes.si/Iscem
Skimleads	http://skimleads.com
Spain	https://sede.registradores.org/contenido/buyingahouse
Spain	http://www.rmc.es/Home.aspx?lang=en
Sweden	http://www.bolagsverket.se
Norway	https://www.brreg.no
Principality of Lichtenstein	http://www.oera.li/hrweb/ger/firmensuche_afj.htm
Switzerland	https://www.zefix.admin.ch/de/search/entity/welcome
United Kingdom	https://www.gov.uk/government/organisations/companies-house

Business Registers (US)

Tool	Link
Alabama	https://sos.alabama.gov
Alaska	https://www.commerce.alaska.gov/CBP/Main
Arizona	http://www.azcc.gov/divisions/corporations
Arkansas	https://www.sos.arkansas.gov/business-commercial-services-bcs
California	http://www.sos.ca.gov
Colorado	http://www.sos.state.co.us
Connecticut	http://portal.ct.gov/sots
Delaware	https://corp.delaware.gov
Florida	http://www.miamidade.gov/businessexpress/start-register.asp
Georgia	http://sos.ga.gov
Hawaii	https://hbe.ehawaii.gov/BizEx/home.eb;jsessionid=FFFC59E1C1F6E7629F05499018074B2B.lana
Idaho	https://sos.idaho.gov
Indiana	http://www.in.gov/sos/business
Illinois	https://www2.illinois.gov/business
Iowa	https://sos.iowa.gov
Kansas	http://www.kssos.org/business/business.html
Kentucky	https://www.sos.ky.gov/Pages/default.aspx
Louisiana	https://www.sos.la.gov/BusinessServices/Pages/default.aspx
Maine	http://www.state.me.us/sos/cec/corp/index.html
Maryland	http://www.dat.state.md.us/Pages/default.aspx
Massachussets	https://www.mass.gov
Michigan	http://www.michigan.gov/business
Minnesota	https://mblsportal.sos.state.mn.us/Business/Search

Mississippi	http://www.sos.ms.gov/Pages/default.aspx
Missouri	https://www.sos.mo.gov/categories.asp?id=2
Montana	http://sos.mt.gov/business
Nebraska	http://www.nebraska.gov/#business
Nevada	https://nvsos.gov/sosentitysearch/corpsearch.aspx
New Hampshire	http://sos.nh.gov/nhbuslookup.aspx
New Jersey	http://www.nj.gov/treasury/revenue/
New Mexico	http://www.tax.newmexico.gov/default.aspx
New York	https://www.dos.ny.gov/
North Carolina	https://www.sosnc.gov/corporations/
North Dakota	https://apps.nd.gov/sc/busnsrch/busnSearch.htm
Ohio	http://business.ohio.gov
Oklahoma	http://www.state.ok.us/?c=4
Oregon	http://sos.oregon.gov/business/Pages/default.aspx
Pennsylvania	https://www.pa.gov
Rhode Island	http://www.ri.gov/business
South Carolina	http://www.scsos.com/Search%20Business%20Filings
South Dakota	http://sdsos.gov/business-services/default.aspx
Tennessee	https://sos.tn.gov/products/business-services/business-information-search-0
Texas	http://www.sos.state.tx.us/corp/index.shtml
Utah	https://corporations.utah.gov
Vermont	http://www.sec.state.vt.us
Virginia	https://www.scc.virginia.gov/index.aspx
Washington	http://access.wa.gov
West Virginia	https://sos.wv.gov/Pages/default.aspx
Wisconsin	http://www.wisconsin.gov/Pages/home.aspx
Wyoming	http://soswy.state.wy.us/Business/Default.aspx

Business Registers (Other)

Tool	Link
Andorra	https://www.ompa.ad
Aruba	http://www.arubachamber.com
Australia	http://www.asic.gov.au
Bahamas	http://www.bahamas.gov.bs/bahamasweb2/home.nsf/vContentW/99B49574E4044661852570180064 7AFB
Bermuda	http://www.roc.gov.bm
British Virgin Islands	http://www.bvifsc.vg
Canada	http://corporationscanada.ic.gc.ca/eic/site/cd-dgc.nsf/Intro
Colombia	http://www.confecamaras.org.co
Curacao	http://www.ruta-curacao.com
Gilbraltar	http://www.companieshouse.gi
Guernsey	http://www.guernseyregistry.com/homepage
India	http://www.mca.gov.in
Isle of Man	https://www.gov.im/categories/business-and-industries/companies-registry
Jersey	http://www.jerseyfsc.org
Malaysia	http://www.ssm.com.my
New Zealand	https://www.business.govt.nz
Philippines	http://www.sec.gov.ph
San Marino	https://www.cc.sm
Serbia	http://www.apr.gov.rs/Default.aspx?alias=www.apr.gov.rs
Singapore	https://www.acra.gov.sg
Sri Lanka	http://www.drc.gov.lk

Thailand	http://www.dbd.go.th/dbdweb_en/ewt_news.php?nid=3974

Business Registers Lists and Directories

Tool	Link
Business Reference Services	http://www.loc.gov/rr/business/company/directories.html
Central and Eastern European Business Directory	http://www.ceebd.co.uk/ceebd
Company Registration Around the World	http://www.commercial-register.sg.ch/home/worldwide.html
Company Research Resources by Country	http://www.rba.co.uk/sources/registers.htm
Europages	https://www.europages.com
European Business Register	http://www.ebr.org
Federation of International Trade Associations	http://www.fita.org/webindex/browse.cgi/Entering_International_Markets/Trade_Information_Business_Directories/international_Business_Directories/Europe_Trade_Directories/All_Europe_Directories
Global Business Register	http://www.globalbusinessregister.com
Global Edge	https://globaledge.msu.edu/global-resources/company-directories
Investigative Dashboard	https://investigativedashboard.org/databases
Knowledge guide to international company registration	http://www.icaew.com/en/library/subject-gateways/business-management/company-administration/knowledge-guide-international-company-registration
List of Company Registers	https://en.wikipedia.org/wiki/List_of_company_registers
Ministry of Economic Development of the Russian Federation	http://www.ved.gov.ru/eng/companies

National Company Registers	https://en.wikipedia.org/wiki/List_of_company_registers
Overseas Company Registers	https://www.gov.uk/government/publications/overseas-registries/overseas-registries
Recoupera	https://recoupera.com/countries-companies-registry
Santander Trade Portal	https://en.portal.santandertrade.com/reach-business-counterparts/business-directories?todo=valider&affichage=&pays_recherche=11&code_secteur=all&tri=#result

Job Search Resources

Tool	Link
Beyond	http://www.beyond.com
CampusCareerCenter	http://www.campuscareercenter.com
CareerBuilder	http://www.careerbuilder.com
College Recruiter	https://www.collegerecruiter.com
Craiglist	http://losangeles.craigslist.org
Dice	http://www.dice.com
Eluta (Canada)	http://www.eluta.ca
Eurojobs	https://www.eurojobs.com
Fish4Jobs	http://www.fish4.co.uk
Gigajob	https://www.gigajob.com
Glassdoor	https://www.glassdoor.com
Headhunter	http://www.headhunter.com
Indeed	http://www.indeed.com
JOBBÖRSE	https://jobboerse.arbeitsagentur.de
JobRobot	https://www.jobrobot.de
Jobs (Germany)	https://www.jobs.de
Jobs (Poland)	http://www.jobs.pl
Jobware (Germany)	https://www.jobware.de
Jobsite (UK)	http://www.jobsite.co.uk
Linkedin	https://www.linkedin.com
Monster	http://www.monster.com
Naukri (India)	http://www.naukri.com
Reed (UK)	http://www.reed.co.uk
Seek (Australia)	http://www.seek.com.au

SimplyHired	http://www.simplyhired.com
Stackoverflow Developer Jobs	https://stackoverflow.com
Stellenanzeigen.de	https://www.stellenanzeigen.de
StepStone	https://www.stepstone.de
whoishiring	https://whoishiring.me
Xing	http://www.xing.com
ZipRecruiter	https://www.ziprecruiter.com

Company Reviews

Tool	Link
CareerBliss Reviews	https://www.careerbliss.com/reviews
Comparably	https://www.comparably.com
Fairygoodbooss	https://fairygodboss.com
Glassdoor	https://www.glassdoor.com
Indeed	https://www.indeed.com/companies
The JobCrowd	https://www.thejobcrowd.com
Jobvoting	https://www.jobvoting.de
Kununu	https://www.kununu.com
LookBeforeYouLeap	http://www.lookbeforeyouleap.net
Meinchef	https://www.meinchef.de
Paysa	https://www.paysa.com
RateMyEmployer	http://www.ratemyemployer.ca
Seek	https://www.seek.com.au/companies
TargetJobs	https://targetjobs.co.uk
Vault	http://www.vault.com

Patent Research

Tool	Link
Advanced Google Patent Search	https://www.google.com/advanced_patent_search
AusPat IP Australia	http://pericles.ipaustralia.gov.au/ols/auspat/welcome.do;jsessionid=GhZjQ0fgjVF4sudf5kQ_8XW5haPebJTu6s55ZIWx6Kh8eh_HzFxk!199765566
Benelux Patent Platform (Belgium, The Netherlands and Luxemburg)	http://mijnoctrooi.rvo.nl/bpp-portal/home
Canada Intellectual Property Office	http://www.ic.gc.ca/opic-cipo/cpd/eng/search/basic.htm l
Common Citation Document FiveIPoffices	http://ccd.fiveipoffices.org/CCD-2.1.6
Danish Patent and Trademark Office	http://www.dkpto.org/online-tools/databases-(free-access).aspx
DPMA Register	https://register.dpma.de/DPMAregister/pat/einsteiger
Espacenet Patent Search (Europe)	https://worldwide.espacenet.com/help?topic=ecla&locale=en_EP&method=handleHelpTopic
European Patent Office	https://register.epo.org/regviewer
Finland Patent Search	https://patent.prh.fi/patinfo/default2.asp?Lng=
Free Patents Online Search	http://www.freepatentsonline.com/search.html
German Patent and Trade Mark Office	https://www.dpma.de/english/search/index.html
Google Patents	https://patents.google.com https://www.google.com/?tbm=pts
GOV.UK Patent Search	https://www.gov.uk/search-for-patent
INPI (France)	https://www.inpi.fr

Israel Patent Authority Database	http://www.ilpatsearch.justice.gov.il/UI/mainpage.aspx
Japan Patent Office	https://www.jpo.go.jp/cgi/linke.cgi?url=/torikumi_e/searchportal_e/classification.htm
Japan Platform for Patent Information	https://www.j-platpat.inpit.go.jp/web/all/top/BTmTopEnglishPage
Korea Intellectual Property Rights Information Service	http://engpat.kipris.or.kr/engpat/searchLogina.do?next=MainSearch
Marcaria Trademark Search	https://trademark-search.marcaria.com
Markenchk	http://www.markenchk.de
Norwegian Industrial Property Office	https://search.patentstyret.no
Office of General Patents (India)	http://ipindia.nic.in
Patent Genius	http://www.patentgenius.com
Patent Search (Spain)	http://consultas2.oepm.es/InvenesWeb/faces/busquedaInternet.jsp
PIZNET	http://www.piznet.de
Swedish Patent and Registration Office	https://www.prv.se/en/patents
Swiss Federal Institute of Intellectual Property	https://www.swissreg.ch/srclient/faces/jsp/start.jsp
UK Intellectual Property Office	https://www.ipo.gov.uk/p-ipsum.htm
United States Patent and Trademark Office (USPTO)	https://www.uspto.gov
USPTO Patent Full-Text and Image Database	http://patft.uspto.gov/netahtml/PTO/search-adv.htm
World Intellectual Property Organization (WIPO)	https://patentscope.wipo.int/search/en/advancedSearch.jsf
World Intellectual Property Organization (WIPO) Hague Express	http://www.wipo.int/designdb/hague/en

Tenders

Tool	Link
APEC Contracting: Tenders and Request for Proposals	https://www.apec.org/Projects/Tenders-and-RFPs
Department of Finance (UK)	https://www.finance-ni.gov.uk/topics/procurement
Development Business	https://www.devbusiness.com/Search/Search.aspx?PreLoadProjects=1
DG Market: Tenders Worldwide	https://www.dgmarket.com
Double Trade	https://www.doubletrade.com
Global Tenders	http://www.globaltenders.com
Infrastructure Civil Works & Construction Tenders	http://www.cwctenders.com
Medical Pharma Healthcare Tenders	http://www.medicaltenders.com/medical_tenders_gcc_countries.htm
Merx (Canada, US)	https://www.merx.com/English/NonMember.asp?WCE=Show&TAB=1&PORTAL=MERX&State=1&hcode=tAF08b5PaGBuUkl43CRDCg%3d%3d
Middle East Tenders Search	http://www.middleeasttenders.com/#20180326108
NSW eTendering	https://tenders.nsw.gov.au
SIMAP Information About European Public Procurement	http://simap.ted.europa.eu
South Australian Tenders & Contracts Website	https://www.tenders.sa.gov.au/tenders/index.do
Tenderio	http://www.tenderio.com
Tenderscope	http://www.tenderscope.com
Tender Link	https://www2.tenderlink.com
Tenders Info	http://www.tendersinfo.com
Tenders Page	https://tenderspage.com

Tenders VIC: Victorian Government Tenders System	https://www.tenders.vic.gov.au/tenders/tender/search/tender-search.do?action=advanced-tender-search-open-tender
The Federation of International Trade Associations	http://www.fita.org/webindex/browse.cgi/Entering_International_Markets/Government_and_Multinational_Procurement/Worldwide_Government_Procurement_Tenders/Europe_Government_Procurement_(Tenders)
Queensland Government Building and Asset Services eTender	https://www.hpw.qld.gov.au/bas/etender
United Nations Development Programme	http://procurement-notices.undp.org/search.cfm
United Nations Global Marketplace	https://www.ungm.org/Public/Notice

Charity, NGO, and Nonprofit Research

Tool	Link
Benefacts (Ireland)	https://benefacts.ie
Benevity Causes Portal	https://causes.benevity.org/causes/search
CAF America	https://cafa.iphiview.com/cafa/givenow/charitydatabasesearch/tabid/464/default.aspx
Charity Commission for England and Wales	https://www.gov.uk/government/organisations/charity-commission
Charity Intelligence	https://www.charityintelligence.ca/research/a-z-charity-listing
Charity Navigator	https://www.charitynavigator.org
Charity Watch	https://www.charitywatch.org
Citizen Audit	https://www.citizenaudit.org
Give.org National Charity Reports	https://give.org/charity-reviews/national
Google Custom Search Engine NGOs Search	https://cse.google.com/cse/home?cx=012681683249965267634:q4g16p05-ao
Government of Canada List of Charities	https://www.canada.ca/en/revenue-agency/services/charities-giving/charities-listings.html
Guide Star	https://www.guidestar.org/NonprofitDirectory.aspx
Illinois Attorney General Charitable Trust Database	http://charitableviewer.ilattorneygeneral.net
IRS Charities & Non-Profits A-Z Site Index	https://www.irs.gov/charities-non-profits/charities-non-profits-a-z-site-index
National Center for Charitable Statistics	http://nccs.urban.org
NYU Libraries NGO, Charity, and Non-Profit Resources	https://guides.nyu.edu/c.php?g=276965&p=1846647

Office of Massachusetts Attorney General Non-Profits & Charities Document Search	http://www.charities.ago.state.ma.us/charities
Open Charities	http://opencharities.org
UK Charity Commission	http://apps.charitycommission.gov.uk/Showcharity/RegisterOfCharities/registerhomepage.aspx
United Nations Department of Economic and Social Affairs NGO Branch	http://esango.un.org/civilsociety/login.do
State of California Department of Justice Charity Research Tool	https://oag.ca.gov/charities/charity-research-tool#Location:Default
Silicon Valley Global Charity Database	https://www.siliconvalleycf.org/ngo
The Chronicle of Philanthropy	https://www.philanthropy.com/data
WANGO Worldwide NGO Directory	http://www.wango.org/resources.aspx?section=ngodir

Real Estate Research

Real Estate Research

Tool	Link
Airbnb	https://www.airbnb.co.uk
Arivify (US)	https://www.arivify.com
Ananz	http://www.ananzi.co.za
Bigger Pockets	https://www.biggerpockets.com/rei
BlueBook International	http://www.bluebook.net
Bret Whissel Amortization Calculator	http://bretwhissel.net/amortization
Carmel Realty Company (CN)	http://www.carmelrealtycompany.cn/real-estate-listings-Carmel.htm
CBRE (Global)	https://www.cbre.us
Central 21 (Global)	https://www.century21.com
Colliers International	https://www2.colliers.com
CouchSurfing	https://www.couchsurfing.com
Digmap Real Estate Tools & Analysis	https://www.digmap.com/solutions/real-estate-analysis
Emporis	https://www.emporis.com
EuroResales	http://www.euroresales.com
FixMyStreet (UK)	https://www.fixmystreet.com
Freddie Mac	http://www.freddiemac.com/research
Funda (NL)	https://www.funda.nl
HomeFacts (US)	https://www.homefacts.com
HomeMetry (US)	https://homemetry.com

HouseShop (UK)	https://www.thehouseshop.com
iLocate (NL)	https://www.ilocate.nl
Institute for Real Estate Management	http://www.irem.org
Jaap (NL)	https://www.jaap.nl
Land.net (US)	http://www.land.net
LondonRentMyHouse	http://www.londonrentmyhouse.com
Loopnet (US)	http://www.loopnet.com
National Association of Realtors Directory of Real Estate Research Centers	https://www.nar.realtor/directories/directory-of-real-estate-research-centers
National Association of Realtors Research Reports	https://www.nar.realtor/research-and-statistics/research-reports
Placester Multiple Listing Service (MLS) Directory (US)	https://placester.com/mls-directory
PadMapper (US)	https://www.padmapper.com
People Looker (US)	https://www.peoplelooker.com
Realestate.com.au (AU)	https://www.realestate.com.au
Real Estate Navigator (US)	https://rehold.com
Realtor	https://www.realtor.com
Redfin (US)	https://www.redfin.com
Rehold (US)	https://rehold.com
Remax Global	https://global.remax.com
RightMove	http://www.rightmove.co.uk
SoldPrice	http://house.speakingsame.com
Sotherby's International Realty	http://www.sothebysrealty.com
SkyscraperPage	http://skyscraperpage.com
Spanish Country Homes (Spain)	http://spanishcountryhomes.com
Street Check (UK)	https://www.streetcheck.co.uk
Total View Real Estate	http://www.totalviewrealestate.com/userguide.php
United Country Real Estate (US)	http://www.unitedcountry.com
US Department of Housing and Urban Development	https://www.hud.gov

World Properties	https://www.worldproperties.com
Zillow (US)	https://www.zillow.com
Zoopla (UK)	https://www.zoopla.co.uk

Online Marketplaces

Classifieds and Online Marketplaces

Tool	Link
2dehands (BE)	https://www.2dehands.be
Alibaba	https://www.alibaba.com
AliExpress	https://www.aliexpress.com
Allegro	https://allegro.pl
Americanas (BR)	https://www.americanas.com.br/hotsite/marketplace-americanas
bedpage	https://www.bedpage.com
Big Commerce Global Marketplaces Index	https://www.bigcommerce.com/blog/global-marketplaces
Bonanza	https://www.bonanza.com
Claz	http://claz.org
Craigslist	https://www.craigslist.org
Depop	https://www.depop.com
ebay	https://www.ebay.com
eBid (Global)	https://www.ebid.net
eCrater	https://www.ecrater.com
Etsy	https://www.etsy.com
Extra (BR, MX)	https://www.extra.com.br/marketplace/venda-no-extra.aspx?origin=ex
FatFingers	http://fatfingers.com
Federal Association of Online Trade Marketplaces Across Europe (DK)	http://bvoh.de/overview-of-online-marketplaces-across-europe

Flipkart (IN)	https://www.flipkart.com
flippity	http://www.flippity.com
Folksy	https://folksy.com
GAME Marketplace (UK)	https://www.help.game.co.uk/hc/en-gb
Goofbay	https://www.hotukdeals.com/deals/goofbay-free-ebay-tools-misspellings-typos-sniper-bargains-1006930
Goofbid	https://www.goofbid.com
Gumtree	https://www.gumtree.com
hotukdeals	https://www.hotukdeals.com
JD (CH)	https://www.jd.com
Jet	https://jet.com
Jingdong Mall (CH)	https://www.jd.com
Jumia (NG)	https://www.jumia.com.ng
Kijiji (Canada)	https://www.kijiji.ca
Lazada (Asia)	https://www.lazada.com
LeoList	https://www.leolist.cc
MarkaVIP (Middle East)	http://markavip.com
Markt.de	https://www.markt.de
Marktplaats	https://www.marktplaats.nl
Mercado Livre (BR, MX)	https://www.mercadolivre.com.br
oodle	https://www.oodle.com
Otto (DE)	https://www.otto.de/unternehmen/en/e-commerce/index.php
OzBargain (AU)	https://www.Ozbargain.com.au
PicClick	https://picclick.com
Privalia (ES, IT, MX, BR)	http://www.privalia.com
Quikr	https://www.quikr.com
Quoka	https://www.quoka.de
Rakuten (JP, DE)	https://www.rakuten.com
Sales Spider	https://www.salespider.com
Search All Junk	http://www.searchalljunk.com
SearchTempest	https://www.searchtempest.com

Shopify	https://www.shopify.com/?utm_source=eCommerce%20platforms&utm_medium=blog&utm_campaign=Pixcblog
Snapdeal (IN)	https://www.snapdeal.com
Speurders	https://www.speurders.nl
Statista Top Real Estate Companies	https://www.statista.com/study/44581/top-100-real-estate-companies
Submarino (BR, MX)	https://www.submarino.com.br
Taobao (CN)	https://www.taobao.com
Tictail	https://tictail.com
TMall (CH)	https://www.tmall.com
Used (Canada)	https://www.used.ca
Willhaben (AT)	http://www.willhaben.at
Zalora (Asia)	https://worldwide.zalora.com
Zibbet	https://www.zibbet.com

Cryptocurrencies and Financial Information

Cryptocurrencies

Tool	Link
Addresswatcher	https://addresswatcher.com
Bitcoin WhosWho	http://bitcoinwhoswho.com
BitRef	https://bitref.com
Blockchain	https://blockchain.info
Block Explorer	https://blockexplorer.com
Blockonomics	https://www.blockonomics.co
Chain Radar	https://chainradar.com
coinbase	https://www.coinbase.com
Crypto Scam Checker	https://fried.com/crypto-scam-checker
Crypto Stack	https://cryptostack.xyz
EtherChain	https://www.etherchain.org
EtherScan	https://etherscan.io
Live Coin Watch	https://www.livecoinwatch.com
Monero Blocks	https://moneroblocks.info
Monero Wallet Hunter	https://www.xmrhunter.com
WalletExplorer	https://www.walletexplorer.com
xmrchain	https://xmrchain.net

Financial Information

Tool	Link
Bin Base	http://www.binbase.com/search.html
Binlist	https://binlist.net
cuitonline	https://www.cuitonline.com
IBAN Check	http://www.tbg5-finance.org/?ibancheck.shtml
IBAN Checker	https://www.iban.com
Search BIN Database	http://www.binbase.com/search.html
TVA Recherche.lu	https://tva-recherche.lu/adresse
VAT Lookup	http://www.vat-lookup.co.uk
VAT Search	http://vat-search.co.uk

Legal Research

Legal Research Reources and Tools

Tool	Link
Asian Legal Information Institute	http://www.asianlii.org
Australian Capital Territory Civil & Administrative Tribunal	http://acat.act.gov.au
Australian Legal Information Institute	http://www.austlii.edu.au
British and Irish Legal Information Institute	http://www.bailii.org
Bundesverfassungsgericht	https://www.bundesverfassungsgericht.de/SiteGlobals/Forms/Suche/Entscheidungensuche_Formular.html
CanLaw (Canada)	https://canlaw.com
CanLII (Canada)	https://www.canlii.org
Cardiff Index to Legal Abbreviations	http://www.legalabbrevs.cardiff.ac.uk
Case Law Database	http://cld.unmict.org
Case Tracker (UK)	http://casetracker.justice.gov.uk
Chambers and Partners	https://www.chambersandpartners.com
Commonwealth Legal Information Institute	http://www.commonlii.org
County-Courts.co.uk	https://county-courts.co.uk
Court Listener	https://www.courtlistener.com
Court News (UK)	http://courtnewsuk.co.uk
Crown Court List (UK)	http://xhibit.justice.gov.uk
Cylaw (Cyprus)	http://www.cylaw.org
De Rechtspraak	https://uitspraken.rechtspraak.nl
Deutsche Justice	http://www.deutschejustiz.de

Droit	http://www.droit.org
DRSP	http://www.drsp.net
Free County Court Records	https://www.blackbookonline.info/USA-County-Court-Records.aspx
Hong Kong Legal Information Institute	http://www.hklii.org
IIJusticia	http://www.iijusticia.edu.ar
Irish Legal Information Initiaitive	https://www.ucc.ie/academic/law/irlii/index.php
ittig	http://www.ittig.cnr.it
Jersey Legal Information Board	https://www.jerseylaw.je
JuraForum	https://www.juraforum.de
Kenya Law	http://kenyalaw.org
Korea Legislation Research Institute	http://www.klri.re.kr
Law Pages	http://www.thelawpages.com
The LAWPHiL Project	https://www.lawphil.net
Law Society (UK)	http://www.lawsociety.org.uk
Law Society of Northern Ireland	https://www.lawsoc-ni.org
Law Society of Scotland	https://www.lawscot.org.uk
Legal Information Institute of India	http://www.liiofindia.org
Legal Tools	http://www.legal-tools.org/en/what-are-the-icc-legal-tools
Legislation.gov.uk	http://www.legislation.gov.uk
Leaxdin	https://www.lexadin.nl/wlg
Lexetius.com	https://lexetius.com
Lexxion	http://www.lexxion.de
Lexum	https://lexum.com
LLRX	https://www.llrx.com
Malawi LII	https://www.malawilii.org
New Zeland Legal Information Institute	http://www.nzlii.org
NYU LIbGuide International Law	http://nyulaw.libguides.com/international-law
OpenJur	https://openjur.de
PACER	https://www.pacer.gov
Pacific Islands Legal Information Institute	http://www.paclii.org

Pinnington Law	https://pinningtonlaw.co.uk
Southern African Legal Information Institute	http://www.saflii.org
Trial International	https://trialinternational.org
UAB Institute of Law and Technology	http://idt.uab.cat
Uganda Legal Information Institute	https://www.ulii.org
UNODC Sherloc	https://www.unodc.org/cld/v3/sherloc
Urteilfinden	http://www.urteilfinden.de
World Legal Information Institute	http://worldlii.org

Researching Countries

Country Profiles

Tool	Link
BBC News Country Profile	http://news.bbc.co.uk/2/hi/country_profiles/default.stm
CIA World Factbook	https://www.cia.gov/library/publications/resources/the-world-factbook/index.html
Country Studies	http://countrystudies.us
Global Edge	https://globaledge.msu.edu
IMUNA Country Profiles	http://www.imuna.org/resources/country-profiles
Kwintessential Country Guides	https://www.kwintessential.co.uk/resources/guides
Library of Congress Country Studies	https://www.loc.gov/collections/country-studies/about-this-collection
Library of Congee Nations	http://www.loc.gov/law/help/guide/nations.php
UN Country Profiles	http://www.un.org/esa/population/publications/countryprofile/profile.htm
UNCTAD Country Profile	http://unctadstat.unctad.org/CountryProfile/en-GB/index.html

Researching Terrorism, Crime, and Cybersecurity

Researching Terrorism

Tool	Link
ALIC Terrorism	https://www.archives.gov/research/alic/reference/terrorism-links.html
Counter Extremism Project	https://www.counterextremism.com
Combating Terrorism Center	https://ctc.usma.edu
Counter Terrorist Trends and Analyses (CTTA)	http://www.rsis.edu.sg/rsis-publication/icpvtr/counter-terrorist-trends-and-analyses-ctta-volume-10-issue-06/#.WyDPZBIzZTZ
Global Counterterrorism Forum	https://www.thegctf.org
Global Terrorism Database	https://www.start.umd.edu/gtd
Global Terrorism Index	https://en.wikipedia.org/wiki/Global_Terrorism_Index#2017
Global Terrorism Research Project	http://gtrp.haverford.edu
International Center for Counter-terrorism	https://icct.nl
Jihadica	http://www.jihadica.com
Online Jihad	https://onlinejihad.net
RAND National Security and Terrorism	https://www.rand.org/topics/national-security-and-terrorism.html
RAND Counterterrorism	https://www.rand.org/topics/counterterrorism.html
Profiles of Individual Radicalization in the United States	http://www.start.umd.edu/data-tools/profiles-individual-radicalization-united-states-pirus

South Asia Terrorism Portal	http://www.satp.org
START Terrorism Databases and Resources	http://www.start.umd.edu/topics/terrorism-databases-and-resources
Terrorism Analysts	http://www.terrorismanalysts.com
Terrorism & Political Violence Risk Map	https://www.riskadvisory.com/campaigns/terrorism-political-violence-risk-map-2018
Tracking Terrorism	https://www.trackingterrorism.org
UN Office of Counter-Terrorism	http://www.un.org/en/counterterrorism/index.shtml
UN Research Counter-terrorism	http://research.un.org/en/counter-terrorism

Researching Crime

Tool	Link
Crime Data Explorer	https://crime-data-explorer.fr.cloud.gov
CrimeReports	https://www.crimereports.com
Data.Police.UK	https://data.police.uk
Europol	https://www.europol.europa.eu
Eurostat Crime	http://ec.europa.eu/eurostat/web/crime/database
International Crimes Database	http://www.internationalcrimesdatabase.org
Interpol	https://www.interpol.int
Office for National Statistics Guide to Finding Crime Statistics	https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/methodologies/guidetofindingcrimestatisticsoct2016
UNODC	http://www.unodc.org
WikiCrimes	http://www.wikicrimes.org

Researching Cybersecurity

Tool	Link
BlackHat	http://www.blackhat.com
Center for Internet Security	https://www.cisecurity.org
CNET Security	https://www.cnet.com/topics/security
Common Weakness Enumeration	http://cwe.mitre.org
CSO Online	https://www.csoonline.com
CVE Details	https://www.cvedetails.com
CVE MITRE	http://cve.mitre.org
Dark Reading	https://www.darkreading.com
DShield	https://dshield.org
Exploit Database	https://www.exploit-db.com
Google Safety Center	https://www.google.com/safetycenter
HelpNetSecurity	https://www.helpnetsecurity.com
Information Systems Security Association International	https://issa.site-ym.com
Infosec Island	http://www.infosecisland.com
Infosecurity Magazine	https://www.infosecurity-magazine.com
Krebs On Security	https://krebsonsecurity.com
Linux Security	http://www.linuxsecurity.com
McAfee Labs	https://securingtomorrow.mcafee.com/mcafee-labs
Microsoft Secure	https://www.microsoft.com/en-us/security/default.aspx
Mozilla Security Blogs	https://blog.mozilla.org/security
Naked Security	https://nakedsecurity.sophos.com
Network World Security	https://www.networkworld.com/category/security

NIST	https://csrc.nist.gov
Packet Storm Security	https://packetstormsecurity.com
SANS	https://www.sans.org
SCMagazine	https://www.scmagazine.com
SecuriTeam	http://www.securiteam.com
Security Focus	https://www.securityfocus.com
Security Intelligence	https://securityintelligence.com
Security Mailing List Archive	http://seclists.org
Security Tube	http://www.securitytube.net
Security Week	https://www.securityweek.com
Security Wizardry Radar	http://www.securitywizardry.com/radar.htm
Stay Safe Online	https://staysafeonline.org/resources
Stop Think Connect	https://stopthinkconnect.org
Talos Intelligence	https://www.talosintelligence.com
Threatpost	https://threatpost.com
Tripwire State of Security	https://www.tripwire.com/state-of-security
US-CERT	https://www.us-cert.gov

Researching Stolen Items

Researching Stolen Items

Tool	Link
Art Loss	http://www.artloss.com
BBB Scam Tracker	https://www.bbb.org/scamtracker/us/
Beds Alert	https://www.bedsalert.co.uk/da/155614/Do_you_recognise_stolen_items_recovered_in_nearby_Hertfordshire_.html
Canadian Police Stolen Property Search	http://www.cpic-cipc.ca/index-eng.htm
Comerica Fraud Center	https://www.comerica.com/fraud-center/report-fraud/lost-stolen-cards-checks.html
Culture Crime News	http://news.culturecrime.org
Find Stolen Art	http://www.findstolenart.com/Search.asp?sr=0
Gestohlen.org	http://www.gestohlen.org
Gumtree Lost & Found	https://www.gumtree.com/lost-found-stuff/uk/stolen
HotGunz	http://www.hotgunz.com
Interpol Works of Art Database	https://www.interpol.int/Crime-areas/Works-of-art/Database
It's BEEN NICKED	http://www.itsbeennicked.co.uk
Pawn Alert	http://www.pawnalert.com/search-stolen-database.html
Prey Project	https://www.preyproject.com
Scrap Theft Alert	https://www.scraptheftalert.com/Home/Home.aspx
Securius	https://www.securius.eu/de/datenbank
Stolen and Found	https://stolenandfound.com
Stolen Boats (UK)	http://www.stolenboats.org.uk

stolencamerafinder	http://www.stolencamerafinder.co.uk
Stolen Caravan, Motorhome and Trailer Tent Database	http://www.ukcampsite.co.uk/articles/view.asp?id=108
Stolen Lost Found	http://www.stolenlostfound.org
Stolen Property	http://www.stolen-property.com
Stolen Register	http://www.stolenregister.com/search
Stolen 911	https://stolen911.com
Trace Checker	https://www.tracechecker.com
The Watch Register	http://www.thewatchregister.com
World Museum Community Red Lists Database	http://icom.museum/resources/red-lists-database

Researching Human Trafficking

Researching Human Trafficking

Tool	Link
Allies Against Slavery	http://www.alliesagainstslavery.org
Asia-Europe Foundation	http://www.asef.org
ASTRA Anti-Trafficking Action	https://www.astra.rs
Arc of Hope for Children	https://arkofhopeforchildren.org/child-trafficking/child-trafficking-statistics
Blue Heart International	http://blueheartinternational.org/human-trafficking-in-california
CARIM East - Consortium for Applied Research on International Migration	http://www.carim-east.eu
Caritas	https://www.caritas.org/what-we-do/migration/human-trafficking
Chance	http://chance.amstat.org
Child Protection Hub	https://childhub.org
CNN Freedom Project	http://thecnnfreedomproject.blogs.cnn.com
Commission on Security and Cooperation in Europe	https://www.csce.gov/issue/human-trafficking
Council of the Baltic Sea States	http://www.cbss.org
Counter-Trafficking Data Collaborative (CTDC)	https://www.ctdatacollaborative.org
Department of Homeland Security Blue Campaign	https://www.dhs.gov/blue-campaign/share-resources
ECPAT	http://www.ecpat.org

Eastern Shore Human Trafficking Task Force	http://eshttf.org
End Slavery Now	http://www.endslaverynow.org
Erase Child Trafficking	https://www.erasechildtrafficking.org
Ethics & religious Liberty Commission Human Trafficking Index	https://erlc.com/resource-library/topic-index/human-trafficking
European Commission	http://ec.europa.eu/anti-trafficking
European Court of Auditors Special Report	http://publications.europa.eu/webpub/eca/special-reports/human-trafficking-09-2017/en
European Freedom Network	http://www.europeanfreedomnetwork.org/resources
Europol	https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/trafficking-in-human-beings
Family and Youth Services Bureau	https://www.acf.hhs.gov/fysb/success-story/trafficking-rhy-20170410
Fight Against Trafficking	https://www.fightagainsttrafficking.org/participating-countries
Force 4 Compassion	http://www.f-4-c.org
Free the Slaves	https://www.freetheslaves.net
Free To Shine	https://www.freetoshine.org
Global Centurion	https://www.globalcenturion.org
Global Incident Map	http://human.globalincidentmap.com
Global Modern Slavery Directory	http://www.globalmodernslavery.org
Global Slavery Index	https://www.globalslaveryindex.org
Human Trafficking Center	http://humantraffickingcenter.org
Human Trafficking Flow Map	http://dataviz.du.edu/projects/htc/flow
Human Trafficking Research	http://humantraffickingsearch.org
Human Rights First	https://www.humanrightsfirst.org
Institute for Security & Development Policy	http://isdp.eu
International Human Trafficking Task Force	http://www.ihttf.com
International Labour Organization	http://www.ilo.org/global/topics/forced-labour/lang--en/index.htm

International Labor Rights Forum	https://www.laborrights.org
International Organization for Migration	https://www.iom.int
International Organization for Migration Australia	http://www.iomvienna.at
Interpol	https://www.interpol.int/Crime-areas/Trafficking-in-human-beings/Trafficking-in-human-beings
Kalamazoo Anti-Human Trafficking Coalition	http://www.kahtc.org
Laboratory to Combat Human Trafficking	https://combathumantrafficking.org/category/research-resources
La Strada International	http://lastradainternational.org
Living For Tomorrow	http://www.lft.ee/human-trafficking
Ludwig Boltzmann Institute: Human Rights	http://bim.lbg.ac.at/en/trafficking-human-beings
Maryland Human Trafficking Task Force	http://www.mdhumantrafficking.org
MTV Staying Alive	http://www.mtvstayingalive.org
National Crime Agency	http://www.nationalcrimeagency.gov.uk/publications/national-referral-mechanism-statistics#
National Human Trafficking Hotline	https://humantraffickinghotline.org
National Society for the Prevention of Cruelty to Children	https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/child-trafficking/research-resources
National Runaway Safeline	https://www.1800runaway.org
Nordic Council of Ministers' Office in Estonia	https://www.norden.ee/en/welfare-society/fight-against-human-trafficking
Not for Sale Campaign	https://www.notforsalecampaign.org
Office for Victims of Crime	https://ovc.ncjrs.gov/humantrafficking/resources.html
Office on Trafficking in Persons	https://www.acf.hhs.gov/otip
Ohio Human Trafficking Task Force	http://humantrafficking.ohio.gov
Pearls4Hope	https://www.pearls4hope.com
Polaris Project	https://polarisproject.org/human-trafficking
Ref World	http://www.refworld.org/cgi-bin/texis/vtx/rwmain

Shared Hope International	https://sharedhope.org/the-problem
Silk Road Studies Program	https://www.silkroadstudies.org
Statista	https://www.statista.com/topics/4238/human-trafficking
Stop the Traffik	https://www.stopthetraffik.org/about-human-trafficking/the-scale-of-human-trafficking
South Carolina Human Trafficking Task Force	http://humantrafficking.scag.gov/data-reports
Thorn	https://www.wearethorn.org/child-trafficking-statistics
United Nations Human Rights Office of the High Commissioner	http://www.ohchr.org/EN/PublicationsResources/Pages/Publications.aspx
USAID	https://www.usaid.gov/trafficking
US Department of Defense Combating Trafficking in Persons	http://ctip.defense.gov
US Department of Health and Human Services Office of Refugee Resettlement	https://www.acf.hhs.gov/orr/trafficking-resources
US Department of Justice Office of Justice Programs - Human Trafficking	https://ojp.gov/specialfocus/humantrafficking/publications.htm
US Department of Justice Child Exploitation and Obscenity Section	https://www.justice.gov/criminal-ceos
US Department of State Office to Monitor and Combat Trafficking in Persons	https://www.state.gov/j/tip
VAW net	https://vawnet.org/sc/human-trafficking
Vets 4 Child Rescue	https://vets4childrescue.org/national-human-trafficking-hotline-statistics

Transportation

Airplanes

Tool	Link
ADS-B Exchange	https://www.adsbexchange.com
Aeroseek	http://www.aeroseek.com
Airmap	https://developers.airmap.com
Airliners	http://www.airliners.net
Airport Webcams	http://airportwebcams.net
Aviation Edge	https://aviation-edge.com/airport-database-api
Avaiation Herald	https://www.avherald.com
Aviation Safety	https://aviation-safety.net
Bridgenet Volans Live Display	http://volans.airportnetwork.com/js3d/volanspublicsfo.html
CAA (UK)	http://www.caa.co.uk
Canadian Civil Aircraft Register	http://wwwapps.tc.gc.ca/saf-sec-sur/2/ccarcs-riacc/RchSimp.aspx
Casper Flights	http://casperflights.com
Donner Radar	http://www.donnyradar.co.uk
FlyAriana (Afghanistan)	http://www.flyariana.com
FlightAware (UK)	https://uk.flightaware.com
FlightAware (US)	https://flightaware.com
Flightradar24	https://www.flightradar24.com
Flight Radar (EU)	https://www.flight-radar.eu
Flight Stats	https://www.flightstats.com

Flightwise	http://flightwise.com
FlightView	https://www.flightview.com
Humberside Airport	https://www.humbersideairport.com/live-flight-information
Open Flights	https://openflights.org/data.html
Opensky Network	https://opensky-network.org
Over the North East	http://www.otne.co.uk/eta
PlaneFinder	https://planefinder.net
Plane Spotters	https://www.planespotters.net
Programmable Web Transportation APIs	https://www.programmableweb.com/category/transportation/api
RadarBox	https://www.radarbox24.com
Radar Virtuel	http://www.radarvirtuel.com
Search Airfields	http://www.pilotweb.aero/airfields/search-airfields
Seatguru	https://www.seatguru.com
Stack Exchange Aviation Forum	https://aviation.stackexchange.com
Symphony Public Vue	https://secure.symphonycdm.com/publicvue/Frames.asp
WebTrak5	http://webtrak5.bksv.com
Zhaw Radar	http://radar.zhaw.ch/AirTraffic.html
360 Radar	https://360radar.co.uk

Drones

Tool	Link
Airdata UAV	https://airdata.com
Australian Government Civil Aviation Safety Authority	https://www.casa.gov.au/aircraft/landing-page/flying-drones-australia
Aviation Safety Network	https://aviation-safety.net/database/issue/drones.php
Bard College Center for the Study of the Drone	http://dronecenter.bard.edu/the-drone-database
Drone no-fly zones	https://kadata.kadaster.nl/dronekaart
dronestagram	http://www.dronestagr.am
Drone Regulations	https://www.droneregulations.info
Drone Research Lab	http://droneresearchlab.com
Drone Wars UK	https://dronewars.net/drone-crash-database
DroneZon	https://www.dronezon.com
Event38	https://event38.com
Federal Aviation Administration	https://www.faa.gov/news/updates/?newsId=85548
Federal Aviation Administration UAS Data on a Map	https://faa.maps.arcgis.com/apps/webappviewer/index.html?id=9c2e4406710048e19806ebf6a06754ad
Global Drone Regulations Database	https://droneregulations.info
Google Map Fusion Table	https://fusiontables.googleusercontent.com/embedviz?viz=MAP&q=select+col2+from+1WuTyH62PmUF97oxo6IreT1BL_aw9HJN5pocwmwg&h=false&lat=44.08758502824518&lng=-85.5615234375&z=4&t=1&l=col2&y=1&tmplt=2
Precision Hawk Mapper	http://www.precisionhawk.com/precisionmapper
RAND Corporation	https://www.rand.org/topics/unmanned-aerial-vehicles.html

Skylark Drone Research	http://www.skylarkdroneresearch.com/skylark-drone-research.html
Skyward	https://skyward.io/support/user-guide/airspace/usa/airports
The Conversation: Drones	http://theconversation.com/us/topics/drones-2513
The Drone Database	http://drones.cnas.org/drones
Travel by Drone	http://travelbydrone.com
UAS Vision	https://www.uasvision.com/about
UAViators Humanitarian UAV Network	http://uaviators.org
United States Association Unmanned Aerial Videography	https://uavus.org
Unmanned Aerial Online	https://unmanned-aerial.com

Cars

Tool	Link
AllVehicleData	http://www.allvehicledata.com
AutoCheck	https://www.autocheck.com/vehiclehistory/?siteID=0
AutoDNA	https://www.autodna.com
AutoTrader (RU)	https://autotraveler.ru/en/spravka/vehicle-registration-codes-in-the-world.html#.Wsz3O4jwY2w
Big Rig VIN	http://bigrigvin.com
Car Detective	https://www.cardetective.com/vin-decoder
CarFax	https://www.carfax.com
Check That VIN	https://checkthatvin.com
FaxVIN	https://www.faxvin.com/vin-check
Federal-Mogul Motorparts Finder	https://www.fmmotorparts.com/fmstorefront/federalmogul/en/USD/catalog/partsFinderLicensePlateLookup
Honda Recall Lookup	https://owners.honda.com/service-maintenance/recalls
Interpol Vehicle Crimes	https://www.interpol.int/Crime-areas/Vehicle-crime/Links
Kelley Blue Book	https://www.kbb.com/vehicle-history-report
License Plates of the World	http://www.worldlicenseplates.com
MOT Checker	https://www.ismycar.co.uk/mot-checker
National Highway Traffic Safety Administration	https://vinrcl.safercar.gov/vin
National Motor Vehicle Title Information System	https://www.vehiclehistory.gov
Reverse Genie License Plate Search	http://www.reversegenie.com/plate.php
Saskatchewan VIN search	https://www.sgi.sk.ca/vin
Vehicle History	https://www.vehiclehistory.com

Vehicle Identification Number	https://vehicleidentificationnumber.com
VINCheck	https://www.nicb.org/how-we-help/vincheck
VINCheck.info	http://vincheck.info
VIN decoder	https://www.vindecoderz.com
VINFree Check	https://www.vinfreecheck.com
VIN Place	http://vin.place

Railways

Tool	Link
ACW Railway (US)	http://www.acwr.com/economic-development/rail-maps
Association of American Railroads	https://www.aar.org
Association for Open Data of Public Transportation Secretariat Office (Japan)	http://airport.odpt.org/index-e.html
Archive Freight Rail Works	http://archive.freightrailworks.org
British Columbia Data Catalogue	https://catalogue.data.gov.bc.ca/dataset/railway-track-line
Canadian Rail Research Laboratory	http://carrl.ca
Centre For Railway Research	http://www.crr.iitkgp.ernet.in/crr/index.php
Data.gov (India)	https://data.gov.in/sector/railways
Data.gov (Saudi Arabia)	http://www.data.gov.sa/en/saudi-railways-organization
Data.gov (US)	https://catalog.data.gov/dataset?tags=railroad
Data.deutschebahn	http://data.deutschebahn.com/dataset
Data.vancouver.ca (Canada)	http://data.vancouver.ca/datacatalogue/railway.htm
DB (Germany)	http://www.apps-bahn.de
DB Open Data Portal	http://data.deutschebahn.com

DSB (Denmark)	https://www.dsb.dk
Eurail (EU) Participating Railway Companies	https://www.eurail.com/en/get-inspired/trains-europe/useful-train-information/participating-railway-companies
European Reference Center for Intermodal Freight Transport	http://eurift.eu/index.php
Federal Railroad Administration (US)	https://www.fra.dot.gov/Page/P0001
Indian Railways	https://railways.socialcops.com
International Association of railway Operations	http://www.iaror.org
International Journal of Railway Research	http://ijrare.iust.ac.ir
Interrail Trains Per Country	https://www.interrail.eu/en/plan-your-trip/trains-europe/trains-country
Intermodal Map (EU)	http://www.intermodal-map.com/freie-karte
Keisei Electric Railway Company (Japan)	http://www.keisei.co.jp
Liik Enne Vira Sto (Finland)	https://www.liikennevirasto.fi/web/en/data
Network Rail (UK)	https://www.networkrail.co.uk/who-we-are/transparency-and-ethics/transparency/open-data-feeds
Odakyu Electric Railway Company (Japan)	https://www.odakyu.jp
Office of Rail and Road (UK)	http://orr.gov.uk/about-orr/corporate-data
Open.cCnada	https://open.canada.ca/data/dataset?keywords=railway+networks
Open Data: City and County of Durham	https://opendurham.nc.gov/explore/dataset/durham-railways
Open Data NI	https://www.opendatani.gov.uk/group/transport

Open Data Peel Region (Canada)	http://opendata.peelregion.ca/data-categories/transportation/railways.aspx
Open Data Regina (Canada)	http://open.regina.ca/dataset/railways
Open Data Swiss	https://opendata.swiss/en/organization/schweizerische-bundesbahnen-sbb
Open Data Transport NSW (Australia)	https://opendata.transport.nsw.gov.au/search/type/dataset
Open Railway Map	https://www.openrailwaymap.org
PennDOT Open Data	https://data-pennshare.opendata.arcgis.com
Queensland Government Data	https://data.qld.gov.au/dataset/steam-locomotive-drawings-and-railway-plans
Rail Analysis India	http://railanalysis.in
Raildar FR	http://raildar.fr
Rail Delivery Group	https://www.raildeliverygroup.com/our-services/rail-data.html
Rail Freight Locations (EU)	http://www.railfreightlocations.eu
Rail Net Europe	http://www.rne.eu/downloads
Railway Gazette	http://www.railwaygazette.com
Railway Research	http://www.railway-research.org
Railway Technical Research Institute	http://www.rtri.or.jp/eng
Railway Technology	https://www.railway-technology.com/company-a-z
Rail Webcams	http://railwebcams.net
Spoorkaart	http://spoorkaart.mwnn.nl
Tobu Railway Company (Japan)	http://www.tobu.co.jp/corporation
Trafa Transport Analysis	https://www.trafa.se/en/rail-traffic
Trafi Finnish Transport Safety Agency	https://www.trafi.fi/en/information_services/open_data
Trainline	https://www.thetrainline.com

Transport Focus (UK)	https://www.transportfocus.org.uk/research-publications/rail-research/#?modes=4
UCL Railway Research Group	http://www.ucl.ac.uk/railway-research
UIC (Union Internationale Des Chemins De Fer)	https://uic.org/research
UK Rail Research and Innovation Network	http://www.ukrrin.org.uk
Union Pacific (US)	https://www.up.com/index.htm
US Department of Transportation Railroads	https://www.transportation.gov/railroads
Welsh Railways Research Circle	http://wrrc.org.uk/research.php
World By Map Railways	http://world.bymap.org/Railways.html

Public Transport

Tool	Link
Bay Area Rapid Transit	http://www.bart.gov
Bureau of Transportation Statistics	https://www.bts.gov
Chicago Regional Transportation Authority	http://data.rtachicago.org
Department for Transport NaPTAN (UK)	http://naptan.dft.gov.uk/naptan/process.htm
DIVA-GIS	http://www.diva-gis.org/gdata
Geofabrik Open Street Map	http://download.geofabrik.de
Global BRT Data	https://brtdata.org
Global Roads Data	http://www.ciesin.columbia.edu/confluence/display/roads/Global+Roads+Data
Global Mass Transit Report	http://www.globalmasstransit.net/archive.php?id=2181
Google Maps - Transit	https://maps.google.com/landing/transit/index.html
Koordinates	https://koordinates.com
Livemap24	https://livemap24.com
Mapnificent	https://www.mapnificent.net
New York City Department of Transportation	http://www.nyc.gov/html/dot/html/about/datafeeds.shtml
Open Cycle Map	https://www.opencyclemap.org
Open Data City of New York	https://opendata.cityofnewyork.us/data
Open Data Platform Swiss Public Transport	https://opentransportdata.swiss/en/dataset

Open Data Showroom	http://opendata-showroom.org/en/traffic
Open Data Soft - Navitia	https://navitia.opendatasoft.com/explore/?sort=modified
Open Data Soft - Navitia	https://navitia.opendatasoft.com/page/start
Open Data Swiss	https://opendata.swiss/en
Open Data Transport (Australia)	https://opendata.transport.nsw.gov.au/dataset/public-transport-realtime-vehicle-positions
Open Street Map	https://www.openstreetmap.org
Open Street Map Belgium	http://www.osm.be
Open Street Map Lithuania	https://openmap.lt/#m/7.34/55.00084/23.95463/0/0
Open Street Map Public Transport Wiki	https://wiki.openstreetmap.org/wiki/Public_transport
ÖPNVKarte (OpenBusMap)	http://www.openbusmap.org
Organisation for Economic Co-operation and Development	https://data.oecd.org/transport/passenger-transport.htm
PT Map	https://ptmap.plepe.at
Public Transport Information (UK)	http://www.carlberry.co.uk/rfnsearch.asp
Public Transport Victoria	https://www.ptv.vic.gov.au/getting-around/maps
Thunderforest Maps	https://www.thunderforest.com/maps
Transitfeeds	http://transitfeeds.com
transitland	https://transit.land/playground
TransitWiki	https://www.transitwiki.org/TransitWiki/index.php/Publicly-accessible_public_transportation_data
Transport for London Open Data	https://tfl.gov.uk/info-for/open-data-users
Transports Metropolitans de Barcelona	https://www.tmb.cat/es/home
Transport Scotland	https://www.transport.gov.scot/public-transport
Traveine	http://www.traveline.info
TRAVIC	http://tracker.geops.ch
Queensland Government Data General Transit	https://data.qld.gov.au/dataset/general-transit-feed-specification-gtfs-qconnect

UITP	http://www.uitp.org/data-statistics
Vision Zero View NYC	http://www.vzv.nyc/#
WikiRoutes	https://wikiroutes.info
World Bank	http://www.worldbank.org/en/topic/transport

Ships

Tool	Link
AIS Data Exchange Dispatcher	http://www.aishub.net/ais-dispatcher
AIS Tracker (Russia)	http://en.aistracker.ru/map7.asp
Arundale	http://arundale.com/docs/ais/sp_map.html
BoatInfoWorld	https://www.boatinfoworld.com
Boat Nerd	http://ais.boatnerd.com
Bottenviken Live AIS	http://ais.sk2hg.se
Coast Guard Vessel Search	https://www.st.nmfs.noaa.gov/coast-guard-vessel-search/index
Cruise Mapper	http://www.cruisemapper.com
Cruise Ship Tracker	http://www.cruisin.me/cruise-ship-tracker
Digimap Guernsey	http://www.digimap.gg/marine/ais
FleetMon	https://www.fleetmon.com
Global Fishing Watch	http://globalfishingwatch.org
Gloucester Harbour Trustees	http://gloucesterharbourtrustees.org.uk/ship-positions-marine-traffic
Helcom AIS	http://maps.helcom.fi/website/AISexplorer
ICC Piracy Map	http://www.icc-ccs.org/piracy-reporting-centre/live-piracy-map
Infomarine	http://www.infomarine24.com
International Registries Inc.	https://www.register-iri.com/index.cfm?action=page&page=53
Krooz Cams	http://www.kroooz-cams.com
Landsort AIS	http://www.landsort-ais.se/aism.html
Live Cruise Ship Tracker	https://www.livecruiseshiptracker.com

Live Cruise Ship Tracker	http://www.thecruisevillage.com/live-cruise-ship-tracker.phtml
Maritime Connector	http://maritime-connector.com
Marine Cadastre	https://marinecadastre.gov/ais
Marine Scotland	http://marine.gov.scot/information/ais-shipping-traffic-selected-ports
MarineTraffic	https://www.marinetraffic.com
MarineTraffic	http://www.marinetraffic.org
My Ship Tracking	https://www.myshiptracking.com
Naxos Island	http://www.naxosisland.eu/live_ship_data.html
Open Sea Map	http://map.openseamap.org
Open Sea Map	http://www.openseamap.org
Pocket Mariner	http://pocketmariner.com
Port Hedland Live AIS	http://www.phseafarers.org/live-ship-map-ais.html
Rathlin Weather AIS (United Kingdom)	http://www.rathlinweather.co.uk/AIS
Sandkilen-Helmi AIS	http://www.helmi.se/en/tours-events/ais-live-trace-7227149
Sandy Bay Yacht Club	http://www.sandybay.org/AIS.shtml
Scanner Net	http://www.scannernet.nl/maritiem/live-ais
SCCOOS (United States)	http://sccoos.org
Shipais	http://www.shipais.com
Ship Finder	http://shipfinder.co
Shipping Explorer	http://www.shippingexplorer.net
ShipSpotting	http://www.shipspotting.com
Ship Tracker Shodan	https://shiptracker.shodan.io
Trewillis.co.uk	http://www.trewillis.co.uk
Vessel Finder	https://www.vesselfinder.com
Vessel Tracker	https://www.vesseltracker.com
World Map	https://worldmap.harvard.edu/maps/2892
World Port Index	https://msi.nga.mil/NGAPortal/MSI.portal?_nfpb=true&_pageLabel=msi_portal_page_62&pubCode=0015
2sandnessjo (Norway)	http://www.2sandnessjo.no/shipplotter/gmap/stavanger.htm l

Container and Cargo Tracking

Tool	Link
APL Tracking	https://www.apl.com/wps/portal/apl/etools/tracking
Cargo Loop	http://www.cargoloop.com
Cargo Tracking	http://cargotracking.utopiax.org/containertracking.html
Container Tracking	http://container-tracking.org
FleetMon	https://www.fleetmon.com/services/container-tracker/search
Freight Metrix	http://www.freightmetrics.com.au/Marine/ShipTracking/tabid/483/Default.aspx
Locus Traxx Worldwide	http://www.locustraxx.com
Marine Traffic	https://www.marinetraffic.com/en/ais/home/centerx:5.7/centery:57.9/zoom:2
My Ship Tracking	https://www.myshiptracking.com
Navipedia	http://www.navipedia.net/index.php/Package_and_Container_Tracking
Searates	https://www.searates.com/container/tracking
Track-trace	http://www.track-trace.com
Vessel Finder	https://www.vesselfinder.com
Vessel Tracker	https://www.vesseltracker.com/en/Googleearth.html

Web Intelligence

Domain and IP Research, Websites Analysis

Tool	Link
Accuranker	https://www.accuranker.com
ahrefs	https://ahrefs.com
Alexa	http://www.alexa.com
altdns	https://github.com/infosec-au/altdns
Analyze ID	http://analyzeid.com
APNIC	https://www.apnic.net
aquatone	https://github.com/michenriksen/aquatone
ARIN	https://www.arin.net
Assetnote-poc	https://github.com/infosec-au/assetnote-poc
Backlink Checker	http://smallseotools.com/backlink-checker
BGP	https://bgp.he.net
Bing Webmaster Tools	http://www.bing.com/toolbox/webmaster
Blacklist Check Tool	http://www.blchecktool.com
BlackWidow	http://www.softbytelabs.com/en/BlackWidow
Blue Backlinks	http://bluebacklinks.com
Bluto-Old	https://github.com/darryllane/Bluto-Old
BotScout	https://botscout.com/search.htm
BrightCloud URL or IP Lookup	https://www.brightcloud.com/tools/url-ip-lookup.php
BuiltWith	http://builtwith.com
Censys	https://censys.io
Central Ops	http://centralops.net

certgraph	https://github.com/lanrat/certgraph
Certificate Search	https://crt.sh
clearwebstats	https://www.clearwebstats.com
CloudFail	https://github.com/m0rtem/CloudFail
CloudFlare Watch	http://crimeflare.biz
Complete DNS	https://completedns.com
COMODO SSL Analyzer	https://sslanalyzer.comodoca.com
Copyscape	http://copyscape.com
Crt.sh	https://crt.sh
CQCounter	http://cqcounter.com/whois
Custom Domain Search Tools	https://inteltechniques.com/osint/menu.domain.html
Custom IP Address Search Tools	https://inteltechniques.com/osint/menu.ip.html
CuteStats	https://www.cutestat.com
Cymon	https://cymon.io
Cymru IP to ASN Lookup	https://asn.cymru.com
Daily Changes	http://dailychanges.domaintools.com
DB-IP	https://db-ip.com
Dedicated or Not	http://dedicatedornot.com
Deepviz - search	https://search.deepviz.com
Denic web whois	https://www.denic.de/webwhois
Digital Point	https://tools.digitalpoint.com
Directory of Malicious IPs	http://www.projecthoneypot.org/list_of_ips.php
DNSDumpster	https://dnsdumpster.com
DNS History	http://dnshistory.org
DNSlytics	https://dnslytics.com
dnspop	https://github.com/bitquark/dnspop
dnsrecon	https://github.com/darkoperator/dnsrecon
DNS Root Instances	https://atlas.ripe.net/results/maps/root-instances
DNSSec Analyzer	https://dnssec-analyzer.verisignlabs.com
DNS Spy	https://dnsspy.io
DNSStuff	http://www.dnsstuff.com
DNS Trails	http://dnstrails.com

DNS Trails	https://securitytrails.com/dns-trails
dnstwister	https://dnstwister.report
DNSViz	http://dnsviz.net
Domain Big Data	http://domainbigdata.com
Domain Crawler	http://www.domaincrawler.com
Domain Dossier	http://centralops.net/co/DomainDossier.aspx
Domain History	http://www.domainhistory.net
Domain & IP Addresses	http://netbootcamp.org/websitetool.html
DomainIQ	https://www.domainiq.com
Domain Tools	https://www.domaintools.com
Domain Tools	http://whois.domaintools.com
downdetector	http://downdetector.com
downforeveryoneorjustme	http://downforeveryoneorjustme.com
DShield API	https://isc.sans.edu/api
EasyCounter WHois	https://whois.easycounter.com
Easy whois	https://www.easywhois.com
EURid	https://eurid.eu
Exfiltrated	http://www.exfiltrated.com/querystart.php
Exonera Tor	https://exonerator.torproject.org
Fierce-domain-scanner	https://github.com/davidpepper/fierce-domain-scanner
FindSubDomains	https://findsubdomains.com
Finitimus	https://chrome.google.com/webstore/detail/finitimus/ckdjcgaagfcnndkkknfmncedapdjaokb?utm_source=chrome-ntp-icon
Follow.net	http://follow.net
gdns	https://github.com/hrbrmstr/gdns
Geo IP Tool	https://geoiptool.com
gobuster	https://github.com/OJ/gobuster
GoDaddy WHois	https://ca.godaddy.com/whois
GooHak	https://github.com/1N3/Goohak
GraphyStories	http://app.graphystories.com
Hexillion	http://hexillion.com
HypeStat	https://www.hypestat.com

Icann Whois	https://whois.icann.org
IKnowWhatYouDownload	https://iknowwhatyoudownload.com/en/peer/?ip=198.8.80.192
InfoBylp (Bulk Domain & IP Lookup	https://www.infobyip.com/ipbulklookup.php
Infosniper	http://www.infosniper.net
intoDNS	http://www.intodns.com
IntelliTamper	http://www.softpedia.com/get/Internet/Other-Internet-Related/IntelliTamper.shtml
InterNIC Whois	http://www.internic.net/whois.html
IP 2 Geolocation	http://ip2geolocation.com
IP 2 Location	https://www.ip2location.com
IP Address	https://www.ip-address.org
IP Address Location	http://www.ipaddresslocation.org
Ipapi Bulk IP Address Lookup	https://app.ipapi.co/bulk
IP Checking	http://www.ipchecking.com
IP Chicken	http://www.ipchicken.com
IP Data	https://ipdata.co
IPFingerprints	http://www.ipfingerprints.com
iphostinfo	https://iphostinfo.com
IP Info	http://ipinfo.info
Ipinfo.io	https://ipinfo.io
ipintel	https://ipintel.io
IP Lists by FireHOL	http://iplists.firehol.org
IP Location	https://www.iplocation.net
IP to ASN	https://iptoasn.com
IP Tracker Online	https://www.iptrackeronline.com
IPv6 Locator	http://ipv6locator.net
ipverse	http://ipverse.net
IPVoid	http://www.ipvoid.com
iTools	http://itools.com
iwantmyname	https://iwantmyname.com
IXMaps Explore	https://www.ixmaps.ca/explore.php

JoeSandboxCloud	https://www.joesandbox.com
Jotti	https://virusscan.jotti.org
Kloth	http://www.kloth.net/services
lacnic	http://www.lacnic.net
Leaked Source	https://leakedsource.ru
Linktally	http://linktally.com
Majestic	https://majestic.com
Maltego	https://www.paterva.com/web7
Malware Domain List	http://www.malwaredomainlist.com/mdl.php
MaxMind	https://www.maxmind.com
McAfee Customer URL Ticketing System	https://trustedsource.org/sources/index.pl
mnemonic	https://passivedns.mnemonic.no
moonsearch	http://moonsearch.com
moreofit	http://www.moreofit.com
Mr. LOOQUER	https://mrlooquer.com
MXToolbox	http://origin.mxtoolbox.com \|\| https://mxtoolbox.com
My IP	https://www.myip.ms
Netcraft Site Report	http://toolbar.netcraft.com/site_report?url=undefined#last_reboot
NetStat Agent	http://netstatagent.com
Network Intelligence	https://netintel.net
Network Tools	http://network-tools.com
Nibbler	http://nibbler.silktide.com
NirSoft	http://www.nirsoft.net
Onyphe	https://www.onyphe.io
OpenLinkProfiler	http://www.openlinkprofiler.org/ratelimit/domain.com
Open Site Explorer	https://moz.com/researchtools/ose
OSINT SPY	https://osint-spy.com
PageGlimpse	http://www.pageglimpse.com
Pentest-Tools Find Subdomains	https://pentest-tools.com/information-gathering/find-subdomains-of-domain
Pentest-Tools.com	https://pentest-tools.com/information-gathering/google-hacking

Plagiarism Checker	http://smallseotools.com/plagiarism-checker
PTRArchive	http://ptrarchive.com
pubDB	http://pub-db.com
Quantcast	https://www.quantcast.com
Quick Sprout	https://www.quicksprout.com
RedirectDetective	http://redirectdetective.com
Remote DNS Lookup	https://remote.12dt.com
Reverse DNS Lookup	https://hackertarget.com/reverse-dns-lookup
Reverse IP to Domain Lookup	http://www.ipfingerprints.com/reverseip.php
RIPE NCC	https://www.ripe.net
RiskIQ	https://community.riskiq.com
Risk Neustar	https://www.risk.neustar/resources/tools/ip-geolocation-lookup-tool
Robtex	https://www.robtex.com
SameID	http://sameid.net
SameIP	http://www.sameip.org
Scamvoid	https://www.scamvoid.com
scanless	https://github.com/vesche/scanless
Scans.io	https://scans.io
Security Headers	https://securityheaders.com
SEMrush	https://www.semrush.com
SEO Chat Tools	http://tools.seochat.com
SEO SiteCheckup Sitemap Test	https://seositecheckup.com/tools/sitemap-test
SEOTools for Excel	http://seotoolsforexcel.com
Serpstat	https://serpstat.com
Shodan	https://www.shodan.io
SIDN	https://www.sidn.nl
Similar Web	https://www.similarweb.com
Site Dossier	http://www.sitedossier.com
Siteliner	http://www.siteliner.com
SiteSleuth	https://www.sitesleuth.io

SmallSEOTools	http://smallseotools.com
Snusbase	https://snusbase.com
Software77 Multi-Lookup	http://software77.net/geo-ip/multi-lookup
SpyCraw	https://www.spycraw.com
SpyOnWeb	http://spyonweb.com
StatsCrop	http://www.statscrop.com
Sublist3r	https://github.com/aboul3la/Sublist3r
Sucuri Free Website and Malware Scanner	https://sitecheck.sucuri.net
Symantec WebPulse Site Review Request	https://sitereview.bluecoat.com
Talos Reputation Lookup	https://talosintelligence.com
TCPIPUTILS.com	http://www.tcpiputils.com
Tejji	http://tejji.com
Threat Crowd	https://www.threatcrowd.org
Threatglass	http://www.threatglass.com
Threat Miner	https://www.threatminer.org
Trend Micro Site Safety Center	https://global.sitesafety.trendmicro.com
Timer4Web	https://www.timer4web.com
Tucows domains	https://www.tucowsdomains.com
urlQuery	http://urlquery.net
urlscan	https://urlscan.io
URLVoid	http://www.urlvoid.com
Utrace	http://en.utrace.de
Verisign	http://dnssec-debugger.verisignlabs.com
Viewdns	http://viewdns.info
Vigilante	https://www.vigilante.pw
Virus Total	https://www.virustotal.com
Visual Site Mapper	http://www.visualsitemapper.com
W3bin.com	https://w3bin.com
W3dt	https://w3dt.net
w3snoop	http://webboar.com.w3snoop.com
Wappalyzer	https://wappalyzer.com

Watch Guard Reputation Authority	http://www.reputationauthority.org
Web Filter Lookup	https://fortiguard.com/webfilter
Web Inspector Free Website Malware Scanner	http://app.webinspector.com
WebMeUp	http://webmeup.com
WebPageTest	https://www.webpagetest.org
Website Informer	http://website.informer.com
Website Outlook	http://websiteoutlook.com
webtarantula	http://webtarantula.com
WhatIsMyIPAddress	http://whatismyipaddress.com
Whois	https://www.whois.com
Who.is	https://who.is
Whois Amped	https://whoisamped.com
Whois Arin Online	https://whois.arin.net
Whois.com	https://www.whois.com
WhoIsHostingThis	http://www.whoishostingthis.com
WHOIS ICANN	https://whois.icann.org
WhoisLookup	http://www.puwong.com/whois
WhoisMind	http://www.whoismind.com
WHOis.net	https://whois.net
Whois.Search	https://whois-search.com
Whoisology	https://whoisology.com
WhoIsRequest	http://whoisrequest.com
WhoLinks2Me	http://www.wholinks2me.com
Whoxy	https://www.whoxy.com
Wigle	https://wigle.net
Woorank	https://www.woorank.com
xray	https://github.com/evilsocket/xray
You Get Signal	http://www.yougetsignal.com
Zulu URL Risk Analyzer	https://zulu.zscaler.com

Web History and Website Capture

Tool	Link
Archive.is	http://archive.is
Archive.fo	http://archive.fo
BlackWidow	http://softbytelabs.com/en/BlackWidow
Cached Pages	http://www.cachedpages.com
Cached View	https://cachedview.nl
Common Crawl	http://commoncrawl.org
Convert Web to PDF	https://play.google.com/store/apps /details?id=com.smobileteam.pdf.activity
Go Back in Time	https://chrome.google.com/webstore/detail /go-back-in-time/hgdahcpipmgehmaaankiglanlgljlakj
InstaWeb	http://www.digiset.me/instaweb
Mass archive	https://github.com/motherboardgithub/mass_archive
PageDash	https://www.pagedash.com
Passive Cache	https://addons.mozilla.org/en-US/firefox/addon/passive-cache
PDFMyURL	http://pdfmyurl.com
Print Friendly	https://www.printfriendly.com
Print What You Like	http://www.printwhatyoulike.com
Resurrect Pages	https://addons.mozilla.org/en-US/firefox/addon/resurrect-pages
Save as PDF Add-on	https://pdfcrowd.com/save-as-pdf-addon
Save to Google Drive	https://chrome.google.com/webstore/detail/save-to-google-drive/gmbmikajjgmnabiglmofipeabaddhgne?hl=en
Save Webpage As Word Document	https://chrome.google.com/webstore/detail/save-webpage-as-word-docu/mcebgdgbcbdkgdljffnkkbekldnidbmn

Screenshots.com	http://www.screenshots.com
Time travel	http://timetravel.mementoweb.org
UK Web Archive	http://www.webarchive.org.uk
Wayback Machine	http://archive.org/web/web.php
Wayback Machine Chrome Add-on	https://chrome.google.com/webstore/detail/wayback-machine/fpnmgdkabkmnadcjpehmlllkndpkmiak?hl=en-US
View-page-archive	https://github.com/dessant/view-page-archive
waybackpack	https://github.com/jsvine/waybackpack
Web2PDF	https://www.web2pdfconvert.com
Web2Pdf.	https://www.microsoft.com/en-us/store/p/web2pdf/9nblgggz5phq
Web Cache	https://chrome.google.com/webstore/detail/web-cache/coblegoildgpecccijneplifmeghcgip
WebCitation	http://webcitation.org/query
Webpage to PDF	http://webpagetopdf.com
Webrecorded	https://webrecorder.io

Wifi Search

Tool	Link
Avast Wifi Finder	https://www.avast.com/en-in/wifi-finder
Find Wifi	https://find-wifi.mylnikov.org
Instabridge	https://instabridge.com
Places to Work	https://placestowork.net
Wifi Finder + Map	https://itunes.apple.com/us/app/map-wifi-wi-fi-finder/id946365975?mt=8&ign-mpt=uo%3D8
Wifi Finder Connect Internet	https://itunes.apple.com/us/app/wifi-finder-free-internet/id1011519183?mt=8&ign-mpt=uo%3D8
WifiFreeSpot	http://www.wififreespot.com
Wigle	https://wigle.net
WikiFiox	https://foxnomad.com/2016/04/26/map-wireless-passwords-airports-lounges-around-world-updated-regularly

Researching Dark Web

Researching Dark Web

Tool	Link
DarkNet Stats	https://dnstats.net
Dark Web Map	https://www.hyperiongray.com/dark-web-map
DeepDotWeb	https://www.deepdotweb.com
DeepWeb Sites	https://www.deepweb-sites.com
DeepWebSitesLinks	https://www.deepwebsiteslinks.com
DarkWebNews	https://darkwebnews.com
Docker-onion-nmap	https://github.com/milesrichardson/docker-onion-nmap
Exonera Tor	https://exonerator.torproject.org
Hidden Wikitor	http://hiddenwikitor.com
Hunchly's Hidden Services Report	https://darkweb.hunch.ly
i2P	https://geti2p.net
onioff	https://github.com/k4m4/onioff
Onion Link	http://onion.link
Onionscan	https://onionscan.org
Onion Investiagtor	https://oint.ctrlbox.com
Onion Land Search Engine	https://onionlandsearchengine.com
Onion Search Engine	http://onionsearchengine.com
The Dark Websites	https://www.thedarkwebsites.com
Tor2Web	https://www.tor2web.org
Tor Netwrok Status	https://torstatus.blutmagie.de
Tor Project	https://www.torproject.org

Torscan	http://torscan.io
Zeronet	https://zeronet.io

Events Search

Events Search

Tool	Link
Eventbrite	https://www.eventbrite.com
Meetup	https://www.meetup.com
WhereEvent	http://www.wherevent.com

Working with Images

Image Search and Reverse Image Search

Tool	Link
Baidu Images	http://image.baidu.com
Berify	https://berify.com
Betaface	https://www.betafaceapi.com
Bing Images	http://www.bing.com/images
Camera Trace	http://www.cameratrace.com/trace
CamFind	https://camfindapp.com
CC Search	https://search.creativecommons.org
Current Location	https://current-location.com
DownloadGram	https://downloadgram.com
Explore Places	http://places2.csail.mit.edu/explore.html
facesearch	http://www.facesaerch.com
FindFace	https://findface.ru
Flickr	https://secure.flickr.com
Flickr Hive Mind	http://flickrhivemind.net
Flickr Map	https://www.flickr.com/map
Fotki	http://www.fotki.com
Geograph	https://www.geograph.org
Google Images	https://images.google.com
Gramfeed	http://www.gramfeed.com
Image Net	http://image-net.org

Image Raider	https://www.imageidentify.com
Imgur	https://imgur.com
KarmaDecay	http://karmadecay.com
Lakako	https://www.lakako.com
Loc.alize.us	https://loc.alize.us
Lycos Images	http://search.lycos.com/images
MyPicsMap	http://www.mypicsmap.com
Photo Map	http://photo-map.ru
PhotoTracker	http://phototracker.ru
Picquery	https://www.picquery.com
Picsearch	http://www.picsearch.com
PicTriev	http://www.pictriev.com
PimEye	https://pimeyes.com/en
Places	http://places2.csail.mit.edu
Reverse GIF	https://ezgif.com/reverse
Reverse Image Search	http://www.reverse-image-search.org
Reverse Image Search	http://www.reverse-image-search.com
Reverse Image Search	https://inteltechniques.com/osint/menu.reverse.image.html
Revimg	http://www.revimg.com
RootAbout	http://rootabout.com
SauceNAO	https://saucenao.com
Small SEO Tools: Reverse Image Search	https://smallseotools.com/reverse-image-search
Smugmug	https://www.smugmug.com/search
Social Catfish Reverse Image Search	https://socialcatfish.com/reverse-image-search
Startpage: Images	https://www.startpage.com/eng/pics.html
StolenCameraFinder	http://www.stolencamerafinder.co.uk
TinyEye	https://tineye.com
Twitter Image Search	https://twitter.com/search?q=%3Csearchterm%3E&src=typd&vertical=default&f=images
View Image	https://chrome.google.com/webstore/detail/view-image/jpcmhcelnjdmblfmjabdeclccemkghjk \|\|

	https://addons.mozilla.org/en-US/firefox/addon/view-image/
Who Stole My Pictures?	https://addons.mozilla.org/en-US/firefox/addon/who-stole-my-pictures
Websta	http://websta.me
Wolfram Language: The Identification Project	https://www.imageidentify.com
Worldcam	http://www.worldc.am
Yahoo Image Search	https://images.search.yahoo.com
Yandex Images	https://www.yandex.com/images

Image Analysis

Tool	Link
AnalogExif	https://sourceforge.net/projects/analogexif
BetaFaceAPI	https://www.betafaceapi.com/demo.html
CameraSummary	https://camerasummary.com
Diffchecker	https://www.diffchecker.com/image-diff
exifdata	http://exifdata.com
Exifer	https://www.thexifer.net
ExifPro	http://www.exifpro.com
Exif Search	http://www.exif-search.com
exiftool	https://sourceforge.net/projects/exiftool
ExifTool by Phil Harvey	http://www.sno.phy.queensu.ca/~phil/exiftool
Exif Viewer	https://chrome.google.com/webstore/detail/exif-viewer/nafpfdcmppffipmhcpkbplhkoiekndck?hl=en
Exif Viewer	https://addons.mozilla.org/en-US/firefox/addon/exif-viewer
Extract Metadata	https://www.extractmetadata.com
Fake Image Detector	https://play.google.com/store/apps/details?id=fake_image_detector.coder.genuine.com.fakeimagedetector&hl=en
FastPreview	https://tn123.org/fastpreview
Find Exif	http://www.findexif.com
Forensically	https://29a.ch/photo-forensics/#level-sweep
FotoForensics	http://www.fotoforensics.com
FourMatch	http://www.fourandsix.com/fourmatch
Fuskr	https://chrome.google.com/webstore/detail/fuskr/glieaboaghdnlglpkekghloldikefofo
Gbimg.org	http://gbimg.org

GeoSetter	http://www.geosetter.de
Ghiro	http://www.getghiro.org
Google Search "View Image" Button	https://chrome.google.com/webstore/detail/google-search-view-image/hgngncnljacgakaiifjcgdnknaglfipo
How Old	https://how-old.net
Image Edited	http://imageedited.com
Image forensic	https://www.imageforensic.org
Image Identification Project	https://www.imageraider.com
Image Search Options	https://addons.mozilla.org/en-US/firefox/addon/image-search-options
Image Verification Assistant	http://reveal-mklab.iti.gr/reveal/index.html
ImgOps	http://imgops.com
ImpulseAdventure	http://www.impulseadventure.com/photo/jpeg-snoop.html
InVID	http://www.invid-project.eu/tools-and-services/invid-verification-plugin
Irfanview	http://www.irfanview.com
izitru	http://www.izitru.com
Java Exif Viewer	https://sourceforge.net/projects/jexifviewer
Jeffrey's Image Metadata Viewer	http://exif.regex.info/exif.cgi
JPEGsnoop	https://github.com/ImpulseAdventure/JPEGsnoop
Let's Enhance	https://letsenhance.io
Logos	http://logos.iti.gr
metapicz	http://metapicz.com/#landing
Photo Detective	https://itunes.apple.com/us/app/photo-detective-pro/id1045128136?mt=8
PhotoMe	http://www.photome.de
Pic2Map	https://www.pic2map.com
Plaghunter	http://www.plaghunter.com
ReadEXIF	https://readexifdata.com
Resemble.js	https://huddle.github.io/Resemble.js
Reveal Image Verification Assistant	http://reveal-mklab.iti.gr/reveal/index.html

RevEye Reverse Image Search	https://chrome.google.com/webstore/detail/reveye-reverse-image-sear/keaaclcjhehbbapnphnmpiklalfhelgf?hl=en
Send to Exif Viewer	https://chrome.google.com/webstore/detail/send-to-exif-viewer/gogiienhpamfmodmlnhdljokkjiapfck?hl=en-US
tawbaware	http://www.tawbaware.com
Veracity (iPhone app)	https://itunes.apple.com/us/app/veracity-image-search/id870153874?mt=8
Verexif	http://www.verexif.com
View Image	https://chrome.google.com/webstore/detail/view-image/jpcmhcelnjdmblfmjabdeclccemkghjk
Web Inspector	https://chrome.google.com/webstore/detail/web-inspector/enibedkmbpadhfofcgjcphipflcbpelf?hl=en
Where is the picture?	https://whereisthepicture.com
Who Stole My Pictures	https://addons.mozilla.org/en-US/firefox/addon/who-stole-my-pictures

Stock Images

Tool	Link
Adobe Stock	https://stock.adobe.com
AlltheFreeStock	http://allthefreestock.com
Burst	https://burst.shopify.com
CC Search Commons	https://ccsearch.creativecommons.org
Clipstill	http://www.clipstill.com
Death to Stock	http://deathtothestockphoto.com
Epicantus	http://epicantus.tumblr.com
Freeimages	http://www.freeimages.com
Freestocks.org	http://freestocks.org
FoodiesFeed	https://www.foodiesfeed.com
Get Refe	http://getrefe.tumblr.com
Getty Images	https://www.gettyimages.com
Gratisography	http://www.gratisography.com
Image Brief	http://www.imagebrief.com
IM Free	http://www.imcreator.com/free
ISO Republic	http://isorepublic.com
iStockphoto	http://www.istockphoto.com
Jay mantri	http://jaymantri.com
Kaboompics	http://kaboompics.com
LibreStock	https://librestock.com
Life of Pix	http://www.lifeofpix.com
Little Visuals	http://littlevisuals.co
MMT	https://mmtstock.com
Moose	https://photos.icons8.com

Morguefile	https://morguefile.com
NegativeSpace	http://negativespace.co
New Old Stock	http://nos.twnsnd.co
Picjumbo	https://picjumbo.com
Picography	https://picography.co
Pixabay	https://pixabay.com
Pexels	https://www.pexels.com
Photobucket	http://photobucket.com
Public Domain Archive	http://publicdomainarchive.com
reshot	https://www.reshot.com
Shot Stash	https://shotstash.com
Shutterstock	http://www.shutterstock.com
skitterphoto	https://skitterphoto.com
SplitShire	https://www.splitshire.com
Startup Stock Photos	http://startupstockphotos.com
StockSnap	https://stocksnap.io
Styled Stock	https://styledstock.co
Superfamous	http://superfamous.com
tookapic	https://stock.tookapic.com
unDraw	https://undraw.co
Unplash	https://unsplash.com

Image and Photo Editing

Tool	Link
AddText+	https://addtext.com
Affinity Photo	https://affinity.serif.com
Annotable	https://itunes.apple.com/us/app/annotable-ultimate-image-annotation/id1099850421?mt=8
Apple Photos	http://www.apple.com/osx/photos
Aviary	https://www.aviary.com
Befunky	https://www.befunky.com
Birme	https://birme.net
Canva	https://www.canva.com
Croppola	http://croppola.com
Ezgif.com	https://ezgif.com
FastSTone	http://www.faststone.org
FlipA Picture	http://flipapicture.com
Fotor	http://www.fotor.com
Foto Flexer	http://fotoflexer.com
Gimp	http://www.gimp.org
Hugin	http://hugin.sourceforge.net
Image Composite Editor	https://research.microsoft.com/en-us/um/redmond/projects/ice/
Image Tricks Lite	https://itunes.apple.com/us/app/image-tricks-lite/id403735824?mt=12
Irfanview	http://www.irfanview.com
LightZone	http://lightzoneproject.org
Lunapic	http://www124.lunapic.com/editor
OnlineImageSplitter	http://www.htmlkit.com/services/is

Paint.NET	http://www.getpaint.net/index.html
Photoscape	http://www.photoscape.org/ps/main/index.php
Photoshop	http://www.photoshop.com
picfull	http://www.picfull.com
PicMoneky	http://www.picmonkey.com
Pixlr	https://pixlr.com
Polarr	https://www.polarr.co
Seashore	http://seashore.sourceforge.net
Social Image Resizer Tool	https://www.internetmarketingninjas.com/seo-tools/favicon-generator-crop-images
SumoPaint	http://www.sumopaint.com
textify	http://textify.it
TinyPNG	https://tinypng.com

OCR Tools

Tool	Link
Free OCR	http://www.free-ocr.com
I2OCR	http://www.i2ocr.com
New OCR	http://www.newocr.com
Online OCR	http://www.onlineocr.net

Working with Videos

Video Search and Reverse Video Search

Tool	Link
360 Daily	http://www.360daily.com
9gag.tv	http://9gag.com/tv
Aol Videos	http://on.aol.com
Bambuser	http://bambuser.com/broadcasts
Berify	https://berify.com
Bing Videos	http://www.bing.com/?scope=video
Crackle	https://www.sonycrackle.com
Custom YouTube Search Tools	https://inteltechniques.com/osint/menu.youtube.html
DailyMotion	http://www.dailymotion.com
DownloadGram	https://downloadgram.com
Download Twitter Video	http://www.downloadtwittervideo.com
Dogpile Video Search	https://www.dogpile.com/?qc=video
D Tube	https://d.tube
Geosearch	http://www.geosearchtool.com
Giphy	https://giphy.com
Google Video Search	https://www.google.com/videohp
Internet Archive: Open Source Videos	https://archive.org/details/opensource_movies
LiveLeak	http://www.liveleak.com
Metacafe	http://www.metacafe.com
Metatube	http://www.metatube.com
MySpace Videos	https://myspace.com/discover/videos

The Open Video Project	https://open-video.org
Reverse Video Search Tools	https://inteltechniques.com/osint/menu.reverse.html
Smugmug	https://www.smugmug.com/search
Snap Map	https://map.snapchat.com
Spaactor	https://www.spaactor.com
Spotter	https://spotter.tech
Startpage Videos	https://www.startpage.com/eng/video.html
TV News Archive	https://archive.org/details/tv
Xplore	http://getxplore.com
Veoh	http://www.veoh.com
Vimeo	https://vimeo.com
Voxalead	http://voxalead.labs.exalead.com
Yahoo Video Search	http://video.search.yahoo.com
Yasiv	http://yasiv.com/youtube
YouTube	https://www.youtube.com
YouTube GeoSearch	http://youtube.github.io/geo-search-tool/search.html

Live Streaming and Webcams

Tool	Link
123webcam	http://123webcam.com
Airport Webcams	http://airportwebcams.net
Bambuser	http://bambuser.com
camvista	http://www.camvista.com
Earthcam	http://www.earthcam.com
Facebook Livemap	https://www.facebook.com/live/map
Flixwagon	http://www.flixwagon.com
Freedocast	http://www.freedocast.com
Insecam	http://www.insecam.org
KeepVid	https://keepvid.com
Krooz Cams	http://www.kroooz-cams.com
Liveleak	https://liveleak.com
Livestream	https://livestream.com
Lookr	https://www.lookr.com
MetaCafe	http://www.metacafe.com
Motorway Cameras	https://www.motorwaycameras.co.uk
OnPeriscope	http://onperiscope.com
OpenStreetCam	https://www.openstreetcam.org
Opentopia	http://www.opentopia.com
Periscope	https://www.periscope.tv
Periscope Map	http://www.periscopemap.live
Periscope Streams	http://onperiscope.com
Perisearch	https://www.perisearch.xyz
PeriViewer	http://periviewer.com

Rail Webcams	http://railwebcams.net
RecPeriscope	http://www.recperiscope.com
Scopedown	http://downloadperiscopevideos.com
See All The Things	https://github.com/baywolf88/seeallthethings
tchannels	https://www.tchannels.tv
Twitch	https://www.twitch.tv
Ustream	http://www.ustream.tv/explore/all
Vaughn Live TV	https://vaughnlive.tv
Vevo	https://www.vevo.com
Vimeo	https://vimeo.com
Webcams Travel	https://www.webcams.travel
WorldCam	https://worldcam.eu
YouNow	https://www.younow.com
YouTube	https://www.youtube.com

Other Video Tools

Tool	Link
Applian	http://applian.com
Avidemux	http://avidemux.sourceforge.net
Clip Converter	https://www.clipconverter.cc
Convertio TS to MP4	https://convertio.co/ts-mp4
Deturl	http://deturl.com
DownFacebook	http://www.downfacebook.com
DownloadHealper	http://www.downloadhelper.net
Download Persicope Videos	http://downloadperiscopevideos.com
Download Subtitle	http://downsub.com
Download Twitter Video	https://www.downloadtwittervideo.com
Downvids.net	http://www.downvids.net
Dredown	http://www.dredown.com
eclips	https://eclips.io
FBDOWN	http://www.fbdown.net
Flash Video Downloader	https://chrome.google.com/webstore/detail/flash-video-downloader/aiimdkdngfcipjohbjenkahhlhccpdbc?hl=de
Format Factory	http://www.pcfreetime.com/formatfactory/index.php
Frame by Frame	https://chrome.google.com/webstore/detail/frame-by-frame-for-youtub/elkadbdicdciddfkdpmaolomehalghio?hl=en-GB
Freemake Video Converter	http://www.freemake.com/free_video_converter/
Free Video Downloader	https://chrome.google.com/webstore/detail/free-video-downloader/ppgadljdflpomdcdacknofppeejgmjdn?hl=de
Handbrake	https://handbrake.fr
hooktube	https://hooktube.com

InVID	http://www.invid-project.eu/tools-and-services/invid-verification-plugin
Invideo for YouTube	https://chrome.google.com/webstore/detail/invideo-for-youtube/iacbjlffnpbhgkgknabhkfmlcpdcigab?
Keep for Chrome	https://chrome.google.com/webstore/detail/keep-for-chrome/ghhhikeonlfpibbaibecmiellnmaikoh
KEEPVID	http://keepvid.com
Logos	http://logos.iti.gr
Montage	https://montage.storyful.com
Orbit Downloader	http://www.orbitdownloader.com
OwlZoom	https://addons.mozilla.org/en-US/firefox/addon/owlzoom-youtube/
Savefrom.net	http://de.savefrom.net
SaveVideo	http://savevideo.me
Softorino YouTube Converter	https://softorino.com/youtube-converter-2
trint	https://trint.com
TubeCHop	http://www.tubechop.com
TWDOWN	https://twdown.net
VDownloader	https://vdownloader.com
Video Downloader Professional	https://chrome.google.com/webstore/detail/video-downloader-professi/elicpjhcidhpjomhibiffojpinpmmpil?hl=de
Video Vault	https://www.bravenewtech.org
VideoVault for Chrome	https://chrome.google.com/webstore/detail/videovault-for-chrome/onoidkfboifjplllldnfnaebfigijckmk
Watch Frame by Frame	http://www.watchframebyframe.com
Y2mate	https://y2mate.com
YooDownload	http://yoodownload.com
Yout	https://yout.com
YouTube Comment Scraper	http://ytcomments.klostermann.ca
YouTube Converter	https://youtubeconvert.cc
YouTube Data Tools	https://tools.digitalmethods.net/netvizz/youtube
YouTube DataViewer	https://www.amnestyusa.org/citizenevidence
Youtube-dl	https://rg3.github.io/youtube-dl
YouTube MP3 Conventer	https://www.ytbmp3.com

YouTube Playlist Analyzer	https://youtube-playlist-analyzer.appspot.com
YouTube Restriction Check	http://polsy.org.uk/stuff/ytrestrict.cgi?ytid=vg7wh_zf2X0
ZamZar TS to MP4	http://www.zamzar.com/convert/ts-to-mp4

Video Editors

Tool	Link
Camtasia	https://www.techsmith.com/video-editor.html
Clip Champ Create	https://clipchamp.com/en/video-editor
DaVinci Resolve	https://www.blackmagicdesign.com/products/davinciresolve
Filmora	https://filmora.wondershare.com
FreeMake	http://www.freemake.com/free_video_converter/?irgwc=1&clickid=wFUzM2U6bT5VXz3zG83eA0TwUkjyvo2GP3k3xA0
Hitfilm Express	https://hitfilm.com/express
iMovie (Mac)	https://www.apple.com/imovie
Kizoa	https://www.kizoa.com/Video-Editor
Lightworks	https://www.lwks.com
Machete	http://www.machetesoft.com
Media 100	https://www.media100.com
Movie Maker Online	http://moviemakeronline.com
NCH Software	http://www.nchsoftware.com/videopad
Online Video Cutter	https://www.wevideo.com
Open Shot Video Editor	https://www.openshot.org
Powtoon	https://www.powtoon.com/home/?
Video Toolbox	http://www.videotoolbox.com
VSCD Free Video Editor	http://www.videosoftdev.com
Wideo	https://wideo.co
WeVideo	https://www.wevideo.com
Windows Movie Maker - Free	https://www.microsoft.com/en-us/store/p/movie-maker-free/9mvfq4lmz6c9

YouTube Video Editor	https://support.google.com/youtube/answer/183851?visit_id=0-636615121384437440-336407512&p=video_editor&hl=en&rd=1

Working with Audio

Radio

Tool	Link
Accuradio	https://www.accuradio.com
AntennaSearch	http://www.antennasearch.com
Antenna Structure Registration Search	http://wireless2.fcc.gov/UlsApp/AsrSearch/asrRegistrationSearch.jsp
Aprs.fi	https://aprs.fi/#!lat=40.51860&lng=-74.34990
ArtSci	http://www.artscipub.com/repeaters
BCC World Service Radio	http://bbcworldservice.radio.net
Broadcastify	http://www.broadcastify.com
Cell Reception	http://www.cellreception.com/towers
City Freq	https://www.cityfreq.com
Digital Frequency Search	https://digitalfrequencysearch.com/index.php
DX Zone	https://www.dxzone.com
HF Underground	https://www.hfunderground.com/board
Home Patrol	http://homepatrol.com
Intercept Radio	http://www.interceptradio.com/bbs
Listenlive	http://www.listenlive.eu
Live365	https://live365.com/listen
Live ATC	https://www.liveatc.net
National Radio Data	http://www.nationalradiodata.com
Police Scanner Info	https://police-scanner.info

Radio.com	https://player.radio.com/station-directory
Radio-locator	https://radio-locator.com
RadioReference	http://www.radioreference.com
Radio Station World	http://radiostationworld.com
Radio Tower	http://radiotower.com
RD Forum	https://www.rdforum.org/index.php
Scanner Master Blog	http://www.scannermasterblog.com/tag/scanner-radio
Streema	https://streema.com
Strong Signals	https://strongsignals.net
TuneIn	https://tunein.com
World Wide DX	https://www.worldwidedx.com/forums/scanning-shortwave-listening.83
Worldwide Radio	http://www.live-radio.net/worldwide.shtml
Zip Scanners	https://www.zipscanners.com/resources/police-scanner-resources-forums-links

Podcasts

Tool	Link
Anchor	https://anchor.fm
Antennapod	http://antennapod.org
BeyondPod	http://www.beyondpod.mobi
Blubrry Podcast Directory	https://create.blubrry.com/resources/blubrry-podcast-directory
Breaker	https://breaker.audio
Castbox	https://castbox.fm
Castro	http://supertop.co/castro
Deepgram	https://www.deepgram.com
Doggcatcher	http://www.doggcatcher.com
Downcast	http://www.downcastapp.com
Edge of the Web Radio	https://edgeofthewebradio.com/seo-podcast
Fyyd	https://fyyd.de
iCatcher! Podcast Player	http://www.joeisanerd.com/apps
iPodder	http://www.ipodder.org
iTunes Podcasts	http://www.apple.com/itunes/podcasts
Listen Notes	https://www.listennotes.com
NPR Podcast Directory	https://www.npr.org/podcasts
Player FM	https://player.fm
Overcast	https://overcast.fm
Pocket Casts	http://www.shiftyjelly.com/pocketcasts
Pocket Casts Voodoo	https://chrome.google.com/webstore/detail/pocket-casts-voodoo/eipnphplecohckkjkgldkmmkgdfbmlek

Podbean	https://www.podbean.com
Podcast App	https://chrome.google.com/webstore/detail/podcast-app/hdpgebcembbojpibjdjbjpnekmabmjmp
Podcast Fast Track	https://podcastfasttrack.com
Podcast Player Prime	https://mybrowseraddon.com/podcast-player.html
Podcast Republic	http://podcastrepublic.net
Podcast Search	http://podcastsearch.david-smith.org
Podcasts	http://www.podcasts.com
Podible	https://podible.co
Podkicker	https://play.google.com/store/apps/details?id=ait.podka&hl=en
podStation Podcast Player	https://chrome.google.com/webstore/detail/podstation-podcast-player/bpcagekijmfcocgjlnnhpdogbplajjfn
PRI SoundWorks	http://www.pri.org/soundworks
Read2me	https://read2me.online
RSSDemon News & Podcast Reader	https://play.google.com/store/apps/details?id=com.meecel.feedreader.RssDemonAd&hl=en
RSS Radio	http://rssrad.io
SmarterPod	https://chrome.google.com/webstore/detail/smarterpod-simple-and-sma/ehlmnfeohfahemdjnakciaheggkojchf
SoundCloud Player	https://chrome.google.com/webstore/detail/soundcloud-player/geamkdoeadoihdcnnkanojmdegppdmkh
SoundCloud Podcasting	https://soundcloud.com/for/podcasting
Spaactor	https://www.spaactor.com
Speaker Podcast Radio	https://www.spreaker.com/download/spreaker-podcast-radio
Stabl	http://www.wearestabl.com
Stitcher	https://www.stitcher.com
The Audacity to Podcast	https://theaudacitytopodcast.com/tap069-top-podcast-directories-and-how-to-get-in-them
tumello	https://tumello.com/search
wecast	http://www.wecastapp.com
Winds	https://getstream.io/winds

Other Audio Tools

Tool	Link
descript	https://www.descript.com
FluidData	https://fluiddata.com
Play.ht	https://play.ht/landing
Rightspeed	https://itunes.apple.com/us/app/rightspeed-the-speed-listening-app/id1104515047?mt=8
Spext	https://www.spext.co
trint	https://trint.com

Working with Documents

Documents and Slides Search

Tool	Link
Ask the EU	https://www.asktheeu.org
Authorstream	http://www.authorstream.com
Court Listener	https://www.courtlistener.com/recap
Custom Document Search by Format	https://inteltechniques.com/osint/docs.format.html
Custom Documents Search Tool	https://inteltechniques.com/osint/docs.html
Declassified and Ratified	http://www.declassifiedandratified.com
DocumentCloud Search	https://www.documentcloud.org/public/search
Edocs-Engine.com	http://www.edocs-engine.com
Find-pdf-doc	http://www.findpdfdoc.com
Free Full PDF	http://www.freefullpdf.com
goofile	https://tools.kali.org/information-gathering/goofile
Hashdoc	https://www.hashdoc.com
Inevstigative Dashboard Search	https://data.occrp.org
Offshore Leak Database	https://offshoreleaks.icij.org
PDF Search Engine	http://www.pdfsearchengine.info
PDFSR	http://pdfsr.com
RECAP	http://archive.recapthelaw.org
Scribd	http://www.scribd.com
SlideSearchEngine	http://www.slidesearchengine.com

SlideShare	http://www.slideshare.net
Slideworld	http://www.slideworld.com
soPDF.com	http://www.sopdf.com

Pastebins

Tool	Link
Custom Pastebin Search	https://inteltechniques.com/osint/menu.pastebins.html
Pastebin	https://pastebin.com
PasteLert	https://andrewmohawk.com/pasteLert
Paste Site Search	http://netbootcamp.org/pastesearch.html

Document and Reference Management

Tool	Link
Colwiz	https://www.colwiz.com
DocumentCloud	https://www.documentcloud.org
Endnote	http://endnote.com
F1000	http://f1000.com
Investigative Dashboard Search	https://data.occrp.org
Mendeley	https://www.mendeley.com
Omnity	https://www.omnity.io
Open Semantic Desktop Search	https://www.opensemanticsearch.org/doc/desktop_search
Overview	https://www.overviewdocs.com
Readcube	https://www.readcube.com
RefME	https://www.refme.com
Zotero	https://www.zotero.org

PDF Management

Tool	Link
CleverPDF	https://www.cleverpdf.com
Foxit Reader	https://www.foxitsoftware.com/products/pdf-reader
ilovepdf	http://www.ilovepdf.com
PDFEscape	https://www.pdfescape.com
PDFExpert	https://pdfexpert.com
PDFx	http://www.metachris.com/pdfx
Smallpdf	http://smallpdf.com
Tabula	http://tabula.technology
Weava Highlighter	https://chrome.google.com/webstore/detail/weava-highlighter-pdf-web/cbnaodkpfinfiipjblikofhlhlcickei
XODO	http://xodo.com
Xpdf	http://www.foolabs.com/xpdf/home.html

Working with Document Metadata

Tool	Link
Doc Scrubber	http://www.brightfort.com/docscrubber.html
ExtractMetadata	http://www.extractmetadata.com
FOCA	https://www.elevenpaths.com/labstools/foca/index.html
Metashield Clean-up-Online	https://metashieldclean-up.elevenpaths.com
OOMetaExtractor	https://archive.codeplex.com/?p=oometaextractor
Pdf-redact-tools	https://github.com/firstlookmedia/pdf-redact-tools
Spiderpig	https://github.com/hatlord/Spiderpig

Academic Resources and Grey Literature

Academic and Grey Literature Research Tools

Tool	Link
Academia	https://www.academia.edu
Academic Index	http://www.academicindex.net
Academic Journals	http://www.academicjournals.org
African Journals Online	http://www.ajol.info
Altmetric	https://www.altmetric.com
American Society of Civil Engineers	http://ascelibrary.org
AMiner	https://aminer.org
Archive	https://archive.org
arXiv	https://arxiv.org
A-Z Library Databases	http://guides.uflib.ufl.edu/az.php
Base	http://www.base-search.net
Beyond Citation	http://www.beyondcitation.org
Bibsonomy	http://www.bibsonomy.org
bioRxiv	https://www.biorxiv.org
Cambridge Journals	http://journals.cambridge.org
Citation Machine	http://www.citationmachine.net
citeulike	http://www.citeulike.org
copac	https://copac.jisc.ac.uk
Core	https://core.ac.uk
deepdyve	https://www.deepdyve.com
Elsevier	https://www.elsevier.com

ERIC	https://eric.ed.gov
EThOS	http://ethos.bl.uk
Etymo	https://etymo.io
Europeana	https://www.europeana.eu
Europe PMC	http://europepmc.org
figshare	https://figshare.com
Focus	https://focus.universite-paris-saclay.fr
The Getty Research Institute	http://www.getty.edu/research/library
Google Scholar	https://scholar.google.com
Google Scholar Button	https://chrome.google.com/webstore/detail/google-scholar-button/ldipcbpaocekfooobnbcddclnhejkcpn
Grey Guide	http://greyguide.isti.cnr.it
Grey Literature (HLWIKI International)	http://hlwiki.slais.ubc.ca/index.php/Grey_literature
Grey Literature – List of Gateways	http://csulb.libguides.com/graylit
Grey Literature Report	http://www.greylit.org
Grey Literature Strategies	http://greylitstrategies.info
GreyNet International	http://www.greynet.org
Hathi Trust Digital Library	https://www.hathitrust.org
HighWire: Free Online Full-text Articles	http://highwire.stanford.edu/lists/freeart.dtl
IEEE Xplore	https://ieeexplore.ieee.org/Xplore/home.jsp
International Affairs Resources	https://internationalaffairsresources.com
IssueLab	https://www.issuelab.org
Journal Guide	https://www.journalguide.com
Journal Seek	http://journalseek.net
JSTOR	http://www.jstor.org
KFF	https://www.kff.org
Lazy Scholar	http://www.lazyscholar.org
Libguides Community	https://community.libguides.com
Library of Congress	https://www.loc.gov
Mednar	https://mednar.com
Microsoft Academic	https://academic.microsoft.com
National Archives	https://www.archives.gov/research/catalog

NRC Research Press	http://www.nrcresearchpress.com
Open Access Scientific Journals	http://www.pagepress.org
OpenAIRE	https://www.openaire.eu
Open DOAR	http://v2.opendoar.sherpa.ac.uk
Open Grey	http://www.opengrey.eu
Open Knowledge Maps	https://openknowledgemaps.org
Open Syllabus Explorer	http://explorer.opensyllabusproject.org
The Open Syllabus Project	http://opensyllabusproject.org
OSF Preprints	https://osf.io/preprints/discover
OSTI.GOV	https://www.osti.gov
Oxford Journals	http://www.oxfordjournals.org
PAGEPress Publications	https://www.pagepress.org
PhilPapers	https://philpapers.org
PLOS	https://www.plos.org
PQDT Open	https://pqdtopen.proquest.com/search.html
PubMed	http://www.ncbi.nlm.nih.gov/pubmed
PubPeer	https://pubpeer.com
Quertle	https://quertle.com
Quetzal Search	https://www.quetzal-search.info
refseek	https://www.refseek.com
Research Gate	http://www.researchgate.net
REPEC	http://repec.org
Retraction Watch	https://retractionwatch.com
SAGE Journals	http://journals.sagepub.com
ScienceDirect	http://www.sciencedirect.com
ScienceDomain	http://www.sciencedomain.org
Science.gov	https://www.science.gov
Science Publications	http://www.thescipub.com
Science Research	http://www.scienceresearch.com
SCIRP	http://www.scirp.org
Scholar Universe	http://www.scholaruniverse.com
Semantic Scholar	https://www.semanticscholar.org
SOC ARXIV	https://osf.io/preprints/socarxiv

Sparrho	https://www.sparrho.com
Springer	http://link.springer.com
SSRN	https://www.ssrn.com
Sweet Search	https://www.sweetsearch.com
Taylor & Francis Online	http://www.tandfonline.com
TechXtra	http://www.techxtra.ac.uk
Unpaywall	https://chrome.google.com/webstore/detail/unpaywall/iplffkdpngmdjhlpjmppncnlhomiipha?hl=en
Video Lectures	http://videolectures.net
Wiley	http://eu.wiley.com
World Digital Library	http://www.wdl.org
World Science	http://worldwidescience.org
zenodo	https://zenodo.org
Zetoc	http://zetoc.jisc.ac.uk

Lectures, Talks, Conference Presentations, Speeches

Lectures, Talks, Conference Presentations, Speeches

Tool	Link
Academic Earth	https://academicearth.org
All Conferences	http://www.allconferences.com
AutoDesk University	http://au.autodesk.com
American Archive of Public Broadcasting	http://americanarchive.org
Brown University Library	https://library.brown.edu
Cornell University Archive	http://societyhumanities.as.cornell.edu/events-archive
Deepgram	https://www.deepgram.com
Elsevier	https://www.elsevier.com/events/conferences
Findlectures	https://www.findlectures.com
Global Academy for Medical Education	https://www.globalacademycme.com/conferences-archive
IEEE Xplore	https://ieeexplore.ieee.org/Xplore/home.jsp
iTunes U	https://itunes.apple.com/us/app/itunes-u/id490217893?mt=8
Kennedy Center Lecture Archive	http://kennedy.byu.edu/lectures
Nature.com	https://www.nature.com/natureevents/science
Nursing Network	https://www.nursingnetwork.com/nursing-events
Open University	http://www.open.ac.uk/#
Renal Archive	http://www.renalarchive.org
Royal Society of Chemistry	http://www.rsc.org/event
Speakerdex	https://speakerdex.co

Streaming Media	http://www.streamingmedia.com/conferences
Talks at Google	https://talksat.withgoogle.com
Ted	https://www.ted.com
The Great Courses	https://www.thegreatcourses.com
UCI School of Social Science	https://www.democracy.uci.edu/resources/asia/index.php

Books and Reading

Books Search and Reading Tools

Tool	Link
100 Million Book	http://www.100millionbooks.org
Amazon Cheap Books	http://www.amazon.com/b?tag=mak041-20&linkCode=as2&ie=UTF8&node=2245146011
Audible	http://www.audible.com
Auditus	https://auditus.cc
Bibliomania	http://www.bibliomania.com
Blinkist	https://www.blinkist.com
Bookbub	https://www.bookbub.com
BookClub	https://bookclub.cool
Bookish	https://www.bookish.com
Booklikes	http://booklikes.com
Bookmate	https://bookmate.com
Bookseer	http://bookseer.com
Books on the Knob	http://blog.booksontheknob.org
Bookstr	https://www.bookstr.com
Calibre	http://www.calibre-ebook.com
Daily Cheap Reads	http://www.dailycheapreads.com
Europeana	https://www.europeana.eu
Favobooks	http://favobooks.com
Free Kindle Books	http://freekindlebooks.org
The Getty Research Institute	http://www.getty.edu/research/library

Gnooks	http://www.gnooks.com
Google Books	https://books.google.com
Goodreads	http://www.goodreads.com
Hathi Trust Digital Library	https://www.hathitrust.org
How Long To Read	https://www.howlongtoreadthis.com
I love my Kindle	https://ilmk.wordpress.com
Internet Archive Texts	http://archive.org/details.php?identifier=texts
ISBN Plus	http://isbnplus.com
Jellybooks	https://www.jellybooks.com
Just Free Books	http://www.justfreebooks.info
Keendly	http://keendly.com
KindleNationDay	http://kindlenationdaily.com
KindleWorld	http://kindleworld.blogspot.com
Lendle	http://lendle.me
LibraryThing	https://www.librarything.com
Librivox	https://librivox.org
Loyal Books	http://www.loyalbooks.com
Many Books	http://manybooks.net
Narro	https://www.narro.co
The Online Books Page	http://digital.library.upenn.edu/books/search.html
Open Culture: Free Audiobooks	http://www.openculture.com/freeaudiobooks
OpeningtheBook	http://www.openingthebook.com
Open Library	https://openlibrary.org
Overdrive	https://www.overdrive.com
ParrotRead	http://parrotread.com
Pixel of Ink	http://www.pixelofink.com
Project Gutenberg	http://www.gutenberg.org
Read	https://medium.com/@readapp/introducing-read-for-ios-de4d2799254a#.z3lrigjr7
Reader IQ	http://www.ereaderiq.com
Readgeek	http://www.readgeek.com
Readism	https://chrome.google.com/webstore/detail/readism-article-reading-t/bmiolhceebkeljaikojgcoeefblcihje

Readlax	https://chrome.google.com/webstore/detail/readlax-speed-reading/noggimpgfjnknjbldfibbdnocffdoii
Readwise	https://readwise.io
Reddit: 52 Weeks, 52 Books	https://www.reddit.com/r/52book
Riffle	https://www.rifflebooks.com
SendtoKindle	https://addons.mozilla.org/en-US/firefox/addon/sendtokindle/?src=search
Talk to Books:	https://books.google.com/talktobooks
TasteDive: Books	https://tastedive.com/books
TheBooksProject	http://thebooksproject.co
TheFrugaleReader	http://www.thefrugalereader.com
The Online Books Page	http://digital.library.upenn.edu/books/search.html
Tinderizer	http://tinderizer.com
Toolinbox Klib	https://en.toolinbox.net/Klib
WhatShouldIReadNext	http://www.whatshouldireadnext.com
YourNextRead	http://www.yournextread.com

Working with Data and Statistics

Data and Statistics

Tool	Link
AGOA Data Center	http://agoa.info
AidData	http://aiddata.org
ADB Statistics and Databases	http://www.adb.org/data/statistics
Archeology Data Service	http://archaeologydataservice.ac.uk
AWS Public Datasets	http://aws.amazon.com/datasets
Bank for International Settlements Statistics	http://www.bis.org/statistics/index.htm
Beyond Citation	http://www.beyondcitation.org
BP Statistical Review of World Energy	http://www.bp.com/en/global/corporate/energy-economics/statistical-review-of-world-energy.html
Berkely Library: Data Lab	http://www.lib.berkeley.edu/libraries/data-lab
Bizstats	http://www.bizstats.com
CIA World Factbook	https://www.cia.gov/library/publications/the-world-factbook
Center for International Earth Science Information Network	http://www.ciesin.org
Center for Global Development	https://www.cgdev.org/commitment-development-index-2017
CEPII	http://www.cepii.fr/CEPII/en/welcome.asp
Data 360	http://www.data360.org
Data BASIC	https://databasic.io
Data Catalog	https://catalog.data.gov/dataset
Data Europa	https://data.europa.eu

Data.gov.uk	https://data.gov.uk
Datawrapper	https://www.datawrapper.de
DBPedia	http://wiki.dbpedia.org
DRYAD	https://datadryad.org
EMBL-EBI	https://www.ebi.ac.uk
European Commission Eurobarometer	http://ec.europa.eu/COMMFrontOffice/PublicOpinion
European Union Open Data Portal	http://open-data.europa.eu/en/data
Eurostat	http://ec.europa.eu/eurostat
FAIRsharing.org	https://fairsharing.org
FAOSTAT	http://faostat3.fao.org
FRED	https://fred.stlouisfed.org
Gapminder World	http://www.gapminder.org/data
globalEDGE Database of International Business Statistics	http://globaledge.msu.edu/tools-and-data/dibs
Google Finance	https://www.google.com/finance
Google Fusion Tables	https://support.google.com/fusiontables/answer/2571232
Google Public Data Explorer	http://www.google.com/publicdata/directory
GOVDATA	https://www.govdata.de
Government of Canada Open Data	http://open.canada.ca/en
IHS Piers	https://www.ihs.com/products/piers.html
Human Development Reports	http://hdr.undp.org/en/global-reports
IDEA Databases	https://www.idea.int/data-tools
International Labour Comparisons	http://www.bls.gov/fls/chartbook.htm
International Trade Center	http://www.intracen.org/ByCountry.aspx
ILOSTAT	https://www.ilo.org/ilostat
ILO World Employment and Social Outlook Trends	http://www.ilo.org/global/research/global-reports/weso/sustainable-enterprises-and-jobs-2017/lang--en/index.htm
IMF Data	http://www.imf.org/en/Data
IMF World Economic Outlook Databases	http://www.imf.org/external/ns/cs.aspx?id=28
Index Mundi	http://www.indexmundi.com
International Energy Agency Energy Atlas	http://energyatlas.iea.org

International Energy Agency Statistics	http://www.iea.org/statistics
Junar	http://junar.com
Knoema	https://knoema.com
LandMatrix	http://landmatrix.org
Latinobarometro	http://www.latinobarometro.org
Library, University of Michigan: Statistics and Datasets	http://www.lib.umich.edu/browse/Statistics%20and%20Data%20Sets
Maptia	https://maptia.com
Nation Master	http://www.nationmaster.com/statistics
OECD Aid Database	http://www.oecd.org/dac/stats/data.htm
OECD Data	https://data.oecd.org
OECD Factbook	http://www.oecd-ilibrary.org/economics/oecd-factbook_18147364
OECD Statistics Directorate	http://www.oecd.org/std
OFFSTATS	http://www.offstats.auckland.ac.nz
Open Data Network	http://www.opendatanetwork.com
Open Data Portal	http://www.opendataportal.at
Open Data Portal Munich	https://www.opengov-muenchen.de
Open Data Showroom	http://opendata-showroom.org
Open Government Data	http://opengovernmentdata.org/data
Paul Hensel's General Informational Data	http://www.paulhensel.org/dataintl.html
Pew Research Center	http://www.pewinternet.org/datasets
Population Reference Bureau Data Finder	http://www.prb.org/DataFinder.aspx
PRS Risk Indicators	http://www.prsgroup.com
Public Open Data Soft	https://public.opendatasoft.com/explore/?sort=modified
Quandl	https://www.quandl.com
Re3data.org	https://www.re3data.org
Research Pipeline	http://www.researchpipeline.com
SESRIC Basic Social and Economic Indicators	http://www.sesric.org/baseind.php
SESRIC Databases	http://www.sesric.org/databases-index.php

Statista	http://www.statista.com
Statpedia	https://statpedia.com
The Atlas of Economic Complexity	http://atlas.cid.harvard.edu
The Data and Story Library	http://lib.stat.cmu.edu/DASL
Trading Economics	http://www.tradingeconomics.com
Transparency.org Corruption Perception Index	https://www.transparency.org/news/feature/corruption_perceptions_index_2016
UK Data Service	https://www.ukdataservice.ac.uk
UN COMTRADE Database	http://comtrade.un.org
UNCTAD Country Fact Sheets	http://unctad.org/en/Pages/DIAE/World%20Investment%20Report/Country-Fact-Sheets.aspx
UNCTAD Investment Country Profiles	http://unctad.org/en/Pages/Publications/Investment-country-profiles.aspx
UNCTAD STAT	http://unctadstat.unctad.org
UN Data	http://data.un.org
UNDP's Human Development Index	http://hdr.undp.org/en/data
UNECE	http://w3.unece.org/PXWeb/en
UNESCO Institute for Statistics	http://www.uis.unesco.org
UNIDO Statistical Databases	http://www.unido.org/resources/statistics/statistical-databases.html
UNStats Social Indicators	http://unstats.un.org/unsd/demographic/products/socind
US Census Bureau	https://www.census.gov
Visual Investigative Scenarios	https://vis.occrp.org
Vizala	https://vizala.com
Upsala Conflict Data Program	http://www.pcr.uu.se/research/UCDP
US Data and Statistics	https://www.usa.gov/statistics
WHO Data	http://www.who.int/gho/en
Wikidata	https://www.wikidata.org
World Bank Data Catalog	https://datacatalog.worldbank.org
World Bank Global Consumption Database	http://datatopics.worldbank.org/consumption/home
World Bank Open Data	http://data.worldbank.org
World Bank Doing Business	http://www.doingbusiness.org

World Bank Enterprise Surveys	http://www.enterprisesurveys.org
World Bank Investing Across Borders	http://iab.worldbank.org
World Integrated Trade Solution	http://wits.worldbank.org
WTO Statistics	https://www.wto.org/english/res_e/statis_e/statis_e.htm
Zanran	http://zanran.com

Infographics and Data Visualization

Tool	Link
Adobe Color CC	https://color.adobe.com/create/color-wheel
Aeon	http://www.aeontimeline.com
Arbor.js	http://arborjs.org
BeakerX	http://beakerx.com
Befunky	https://www.befunky.com
Bizint	http://www.bizint.com
Cacoo	https://cacoo.com
Canva	https://www.canva.com
chartblocks	http://www.chartblocks.com
Charted	http://www.charted.co
Chartico	http://chartico.com
Chart.js	http://www.chartjs.org
Circos	http://circos.ca
creately	http://creately.com
Crossfilter	http://square.github.io/crossfilter
csvkit	https://github.com/wireservice/csvkit
DataBasic.io	https://databasic.io
Data Visualization Catalogue	http://datavizcatalogue.com
D3js	https://d3js.org
Datawrapper	https://datawrapper.de
dygraphs	http://dygraphs.com
easely	http://www.easel.ly
Exhibit	http://www.simile-widgets.org/exhibit
Flot	http://www.flotcharts.org

FusionCharts	http://www.fusioncharts.com
Google Developers: Charts	https://developers.google.com/chart
Google Fusion Tables	https://support.google.com/fusiontables/answer/2571232
GraphX	http://spark.apache.org/graphx
Highcharts	http://www.highcharts.com
Hohli	http://charts.hohli.com
Inkscape	https://inkscape.org
Infogr.am	https://infogr.am
Java Infovis Toolkit	http://philogb.github.io/jit
JpGraph	http://jpgraph.net
jqPlot	http://www.jqplot.com
Knoema	https://knoema.com
Leaflet	http://leafletjs.com
Listify	http://listify.okfnlabs.org
Linkuroius	http://linkurio.us
Lucidchart	https://www.lucidchart.com
Neo4j	https://neo4j.com
Nodebox	https://www.nodebox.net
OpenLayers	http://openlayers.org
Palladio	http://hdlab.stanford.edu/palladio
Piktochart	https://piktochart.com
Pixcone	http://www.pixcone.com
Pixxa	http://www.pixxa.com
Plotly	https://plot.ly
Sizzle	https://www.sizzleanalytics.com
SpicyNodes	http://www.spicynodes.org
QlikView	https://www.visualintelligence.co.nz/qlikview
Quadrigram	http://www.quadrigram.com
Raphael	http://dmitrybaranovskiy.github.io/raphael
RAW Graphs	http://app.rawgraphs.io
Shanti Interactive	http://www.viseyes.org
Snappa	https://snappa.io
Statpedia	http://statpedia.com

Tableau	http://www.tableau.com
Tableau Public	https://public.tableau.com
Textures.js	https://riccardoscalco.github.io/textures
Tiki-toki	http://www.tiki-toki.com
Tik-tok	https://datanews.github.io/tik-tok
Timeflow	https://github.com/FlowingMedia/TimeFlow/wiki
Timeglider	http://timeglider.com/widget
Timeline	http://timeline.knightlab.com
Timeline	http://www.simile-widgets.org/timeline
Timeline Maker	https://www.timelinemaker.com
Timetoast	http://www.timetoast.com
Word Art	https://wordart.com
Wordle	http://www.wordle.net
Venngage	https://venngage.com
Visage	https://visage.co
Vis.js	http://visjs.org
Visme	http://www.visme.co
Visual Investigative Scenarios	https://vis.occrp.org
Visualize.me	http://vizualize.me
visually	https://visual.ly
Vortex	http://www.dotmatics.com/products/vortex
ZingChart	http://www.zingchart.com

Dashboard Tools

Tool	Link
Analytics Portfolio	https://analyticsportfolio.com
Chartio	https://chartio.com
Clicdata	http://www.clicdata.com
Cyfe	http://www.cyfe.com
Dashthis	https://dashthis.com
DataDeck	https://www.datadeck.com
Geckoboard	https://www.geckoboard.com
Happy Metrics	https://www.happymetrix.com
Klipfolio	http://www.klipfolio.com
Qlik	http://www.qlik.com
Visually	http://visual.ly

Data Analysis

Tool	Link
Automatic Statistician	https://www.automaticstatistician.com
Auto-WEKA	http://www.cs.ubc.ca/labs/beta/Projects/autoweka
AW Stats	http://www.awstats.org
bigML	https://bigml.com
Cloud Automl	https://cloud.google.com/automl
Countly	https://count.ly/web-analytics
DataCracker	https://www.datacracker.com
Dataiku DSS	https://www.dataiku.com/dss/trynow
Data Kleenr	http://chi2innovations.com/datakleenr
Data Pine	https://www.datapine.com/data-analysis-tools
Data Preparator	http://www.datapreparator.com
DataRobot	https://www.datarobot.com
Data Wrapper	https://www.datawrapper.de
Data Wrangler	http://vis.stanford.edu/wrangler
D3	https://d3js.org
eAnalytics	http://www.eanalytics.de
Exhibit	http://simile-widgets.org/exhibit
Exmerg	http://www.exmerg.com
Google Analytics	https://www.google.com/analytics/?gclid=CjwKEAiAh7WkBRCQj-_zwZvk52ISJADj7z8COo_vM67BKDQAuisEzPwsNZ5Yphpu7Q5x2MirmakiUxoCZ6fw_wcB#?modal_active=none
Google Data Studio	https://www.google.com/analytics/data-studio
Google Fusion Tables	https://support.google.com/fusiontables/answer/2571232
H2O.ai	https://www.h2o.ai

Import.io	https://www.import.io
JavaScript InfoVis Toolkit	http://philogb.github.io/jit
Knime Analytics Platform	https://www.knime.com/knime-analytics-platform
Matomo	https://matomo.org
Microsoft Azure Machine Learning Studio	https://studio.azureml.net
MLBase	http://mlbase.org
MLJAR	https://mljar.com
Mr. Data Converter	https://shancarter.github.io/mr-data-converter
OpenRefine	https://github.com/OpenRefine
Open Web Analytics	http://www.openwebanalytics.com
Orange	https://orange.biolab.si
Paxata	https://www.paxata.com
PDF Tables	https://pdftables.com
Public Open Data Soft	https://public.opendatasoft.com/explore/?sort=modified
Rapid Miner	https://rapidminer.com
R Project	https://www.r-project.org
Scumblr	https://github.com/Netflix/scumblr/wiki
SEM Rush	https://www.semrush.com
Tableau Public	https://public.tableau.com/s
Talend	https://www.talend.com/products/data-preparation#free-desktop
Trifacta	https://www.trifacta.com
Weka	https://www.cs.waikato.ac.nz/ml/weka
Zoho Reports	https://www.zoho.com/reports
Qlik View	http://global.qlik.com/us/landing/go-sm/qlikview/download-qlikview

Data Scrapers

Tool	Link
Agenty	https://www.agenty.com
Beautiful Soup	https://www.crummy.com/software/BeautifulSoup/bs4/doc
Big Data Made Simple	http://bigdata-madesimple.com/top-50-open-source-web-crawlers-for-data-mining
Cola	https://github.com/chineking/cola
Content Bomb	http://www.contentbomb.com
Connotate	https://www.connotate.com
Common Crawl	https://commoncrawl.org
Crawly	http://crawly.diffbot.com
Crawl Monster	https://www.crawlmonster.com
Cyotek WebCopy	https://www.cyotek.com/cyotek-webcopy
Data Miner	https://data-miner.io
Demiurge	https://github.com/matiasb/demiurge
Dexi.io	https://dexi.io
DiffBot	https://www.diffbot.com
FMiner	http://www.fminer.com
Getleft	https://sourceforge.net/projects/getleftdown
Grabby	https://grabby.io
Helium Scraper	http://www.heliumscraper.com/en/index.php?p=home
HTTrack	https://www.httrack.com
Import.io	https://www.import.io
Lassie	https://github.com/michaelhelmick/lassie
Listly	https://listly.io

Mechanical Soup	https://github.com/MechanicalSoup/MechanicalSoup
Octoparse	https://www.octoparse.com
Open Data Tools	http://opendata-tools.org/en/data
OutWit Docs	http://www.outwit.com/products/docs
OutWit Hub	http://www.outwit.com/products/hub
Parsehub	https://www.parsehub.com
Portia	https://scrapinghub.com/portia
Pyspider	https://github.com/binux/pyspider
Reaper	https://reaper.social \|\| https://github.com/ScriptSmith/reaper/blob/master/README.md
Scraper	https://chrome.google.com/webstore/detail/scraper/mbigbapnjcgaffohmbkdlecaccepngjd
Scraper Wiki	https://scraperwiki.com
Scrapy	https://scrapy.org
Screen Scraper	https://www.screen-scraper.com
Sitebulb	https://sitebulb.com
UiPath	https://www.uipath.com/community
Web Harvy	https://www.webharvy.com
Webhose.io	https://webhose.io
Web Scraper	http://webscraper.io
80 Legs	http://80legs.com

Working with News

News Sources

Tool	Link
1st Headlines	http://www.1stheadlines.com
ABYZNewsLinks	http://www.abyznewslinks.com
AllYouCanRead	http://www.allyoucanread.com
AP	http://hosted.ap.org
Associated France Press (AFP)	http://www.afp.com
BBC News	http://www.bbc.co.uk/news
Bing News	http://www.bing.com/news
CNN	http://edition.cnn.com
DailyEarth	http://dailyearth.com
DPA International	http://www.dpa-international.com
The Economist Explorer	https://yvoschaap.com/economist
EMM	http://emm.newsbrief.eu/NewsBrief/clusteredition/en/latest.html
Euronews	http://www.euronews.com
Europe Media Monitor (EMM) NewsExplorer	http://emm.newsexplorer.eu
Factiva	http://www.dowjones.com/factiva
France24	http://www.france24.com
Good Gopher	http://www.goodgopher.com
Google News	https://news.google.com
Google News Print Archive	http://news.google.com/newspapers
HeadlineSpot	http://www.headlinespot.com

Inshorts	https://inshorts.com/en/read
Itar-Tass	http://www.itar-tass.com
Library of Congress – US Newspapers	http://chroniclingamerica.loc.gov/search/titles \|\| http://chroniclingamerica.loc.gov
MagPortal	http://www.magportal.com
NewsBot	https://getnewsbot.com
News Map	http://newsmap.jp
News Now	http://www.newsnow.co.uk
Newseum - Today Front Pages	http://www.newseum.org/todaysfrontpages
NewsLookup	http://www.newslookup.com
Newsography	http://newsography.com
Newspaper Map	http://newspapermap.com
Newspaperindex	http://www.newspaperindex.com
Newspapers.com	http://www.newspapers.com
OnlineNewspapers	http://www.onlinenewspapers.com
Paperboy	http://www.thepaperboy.com
Patch	https://patch.com/map
PR Newswire	http://www.prnewswire.com
Press Reader	http://www.pressreader.com
Reuters	http://www.reuters.com
Silobreaker	http://www.silobreaker.com
storyzy	http://search.storyzy.com
TV News Archive	https://archive.org/details/tv
Wikinews	https://en.wikinews.org
Wikipedia: Current Events	https://en.wikipedia.org/wiki/Portal:Current_events
WorldNews	http://wn.com
World-Newspapers	http://www.world-newspapers.com
Yahoo News	http://news.yahoo.com
YouGotTheNews.com	http://yougotthenews.com

News Digest and Discovery Tools

Tool	Link
10000 Flies	http://www.10000flies.de
anderpink	https://anderspink.com
Banjo	https://ban.jo
Blende	https://launch.blendle.com
FastNews	https://fastnews.me
Flipboard	https://flipboard.com
Hubii	http://hubii.com
inkl	https://www.inkl.com
inshorts	https://www.inshorts.com
[INSIDE]	http://blog.inside.com
News360	https://news360.com
NewsBot	https://getnewsbot.com
News Explorer	https://betamagic.nl/products/newsexplorer.html
Nuzzle	http://nuzzel.com
Populast	http://populast.com
Press Reader	http://www.pressreader.com
Reality Brief	http://www.realitybrief.com
Reeder	http://reederapp.com
SmartNews	https://www.smartnews.com
Spike	http://www.newswhip.com
Superdesk	https://www.superdesk.org
TLDR World News	https://tldrworldnews.com
Topix	http://www.topix.com

Fact Checking

Tool	Link
AfricaCheck	https://africacheck.org
AIDR	http://aidr.qcri.org
Check	https://meedan.com/en/check
Checkdesk	https://meedan.com/en/checkdesk
Chequeado	http://chequeado.com
Citizen Desk	https://www.sourcefabric.org/en/citizendesk
CivikOwl	http://www.civikowl.com
Emergent	http://www.emergent.info
Fact Check	http://www.factcheck.org
Fakespot	https://www.fakespot.com
FirstDraftNews Check	https://chrome.google.com/webstore/detail/firstdraftnewscheck/japockpeaaanknlkhagilkgcledilbfk
Full Fact	https://fullfact.org
Hoaxy	https://hoaxy.iuni.iu.edu
InVID	http://www.invid-project.eu/tools-and-services/invid-verification-plugin
MediaBugs	http://mediabugs.org
Reporterslab Fact Checking	https://reporterslab.org/fact-checking
Snopes	http://www.snopes.com
StopFake	http://www.stopfake.org/en/news
Truly	http://www.truly.media
Trusted News	https://trusted-news.com
TrustServista	https://www.trustservista.com
Urban Legends	https://www.thoughtco.com/urban-legends-4132595

Verificado	https://verificado.mx
Verification Handbook	http://verificationhandbook.com
Verification Junkie	http://verificationjunkie.com
Verification Checklist	https://revealproject.eu/a-roadmap-to-the-truth
Verify Syria	http://www.verify-sy.com/en

Working with Foreign Language Content

Translation Tools

Tool	Link
2lingual	http://www.2lingual.com
Apertium	https://www.apertium.org
Babelfish	https://www.babelfish.com
Bab.la	https://en.bab.la
Bablic	https://www.bablic.com
Babylon	http://translation.babylon.com
Bing Translator	http://www.bing.com/translator
British Slang	http://www.britishslang.co.uk
Deepl Translator	https://www.deepl.com/translator
Dict.cn	http://dict.cn
Dictionary.com: Translation	http://translate.reference.com
FreeTranslation	http://www.freetranslation.com
Free Translator	http://www.free-translator.com
Free Website Translation	http://free-website-translation.com
Frengly	http://frengly.com
Gengo	http://gengo.com
Gizoogle	http://gizoogle.net/textilizer.php
Google Input Tools	https://www.google.com/inputtools/try
Google Translate	https://translate.google.com
Google Translate Extension	https://chrome.google.com/webstore/detail/google-translate/aapbdbdomjkkjkaonfhkkikfgjllcleb?hl=en
IdiomaX Translation	http://www.idiomax.com/online-translator.aspx

imTranslator	http://imtranslator.net/translation
India Typing	http://indiatyping.com/index.php/translations/english-to-hindi-translation
Irish Translator	http://www.whoohoo.co.uk/irish-translator.asp
iTranslate	https://www.itranslate.com
iTranslate Voice	http://itranslatevoice.com
Lexicool Translation	http://www.lexicool.com/translate.asp
Lexilogos	https://www.lexilogos.com
Linguee	http://www.linguee.com
LingvoSoftOnline	http://www.lingvozone.com
Microsoft Translator	http://www.microsoft.com/en-us/translator
Noslang	http://www.noslang.com
OdysseyTranslator	http://odysseytranslator.com
Online Translator	http://www.online-translator.com
Pleco	https://www.pleco.com
PROMT-Online	http://translation2.paralink.com
Reddit/r/translator	https://www.reddit.com/r/translator
Reverso	http://www.reverso.net
Reverso Dictionary	https://dictionary.reverso.net
Sco Translate	http://www.scotranslate.com
Slangit	http://slangit.com
Spanish Dict	http://www.spanishdict.com
South African Slang	http://www.rsa-overseas.com/features/slang.htm
Systran	http://www.systransoft.com
Trans8it	http://transl8it.com
Translate British	https://www.translatebritish.com
Translate.com	https://www.translate.com
Translation2	http://translation2.paralink.com
Unbabel	https://unbabel.com
Urban Dictionary	https://www.urbandictionary.com
Wiktionary	https://www.wiktionary.org
WorldLingo	http://www.worldlingo.com
WorldReference.com	http://www.wordreference.com

Yamli (Arabic Search Engine)	http://www.yamli.com
Yandex Translate	https://translate.yandex.ru

Web Monitoring

RSS Readers

Tool	Link
Awasu	http://www.awasu.com
Cappuccino	http://cappuccinoapp.com
CurioStudio	http://www.curiostudio.com
DiggReader	http://digg.com/login?next=%2Freader
Fedora Reeder	https://www.microsoft.com/en-us/store/p/fedora-reader/9nblgggzm828?ranMID=24542&ranEAID=TnL5HPStwNw&ranSiteID=TnL5HPStwNw-f3VMyJK1Njf8DUSG_atALQ&tduid=(e939f887862d0b3f3ccbf2a2fb27c10c)(256380)(2459594)(TnL5HPStwNw-f3VMyJK1Njf8DUSG_atALQ)()
Feedafever	http://www.feedafever.com
FeedDemon	http://www.feeddemon.com
Feedenlarger	http://feedenlarger.com
Feedly	http://www.feedly.com
FeedReader	http://www.feedreader.com
Netvibes	http://www.netvibes.com
Newsblur	http://newsblur.com
Nextgen Reader	https://www.microsoft.com/en-us/store/p/nextgen-reader/9wzdncrfj262?ranMID=24542&ranEAID=TnL5HPStwNw&ranSiteID=TnL5HPStwNw-RfRFLElSGFCdyaiTXT53gg&tduid=(e939f887862d0b3f3ccbf2a2fb27c10c)(256380)(2459594)(TnL5HPStwNw-RfRFLElSGFCdyaiTXT53gg)()
OmeaReader	http://www.jetbrains.com/omea/reader

Pine	https://pine.blog
QuiteRSS	https://quiterss.org
Royal	http://www.the-sz.com/products/royal
RSS Bridge	https://github.com/RSS-Bridge/rss-bridge
RSS Feed Reader	https://chrome.google.com/webstore/detail/rss-feed-reader/pnjaodmkngahhkoihejjehlcdlnohgmp
RSS for the rest of us	https://github.com/wilderborn/rss-for-the-rest-of-us
RSSOwl	http://www.rssowl.org
Rufus	https://github.com/jtanza/rufus
Telescope	https://itunes.apple.com/us/app/telescope-news-rss-reader/id1353282977?mt=8
Selfoss	http://selfoss.aditu.de
The Old Reader	http://theoldreader.com
ViennaRSS	https://github.com/ViennaRSS/vienna-rss
Winds	https://getstream.io/winds

Other RSS Tools

Tool	Link
Bridge.Leslibres	https://bridge.leslibres.org
Bridge.Suumitsu	https://bridge.suumitsu.eu
Feed Filter Maker	http://feed.janicek.co
Fetch RSS	http://fetchrss.com
Google Alerts	http://www.google.com/alerts
Google-alerts 0.1.5	https://pypi.org/project/google-alerts
Kill the Newsletter	https://www.kill-the-newsletter.com
Pipes	https://www.pipes.digital
Reeder	http://reederapp.com
RSS Bridge	https://github.com/RSS-Bridge/rss-bridge
RSS Micro	http://www.rssmicro.com
RSS Search Hub	http://www.rsssearchhub.com
RSS Subscription Extension	https://chrome.google.com/webstore/detail/rss-subscription-extensio/bmjffnfcokiodbeiamclanljnaheeoke?hl=en
Sage	https://addons.mozilla.org/en-US/firefox/addon/sage/?src=search
siftrss	https://siftrss.com

Website Monitoring

Tool	Link
ChangeDetect	http://www.changedetect.com
ChangeTower	https://changetower.com
Custodee	https://www.custodee.com
deltafeed	http://bitreading.com/deltafeed
Distil Web Monitor	https://chrome.google.com/webstore/detail/distill-web-monitor/inlikjemeeknofckkjolnjbpehgadgge?hl=en-US
Feed43	http://feed43.com
FollowThatPage	http://www.followthatpage.com
OnWebChange	http://onwebchange.com
urlwatch	https://github.com/thp/urlwatch
versionista	http://versionista.com
visualping	https://visualping.io
WatchThatPage	http://www.watchthatpage.com
WebSite Watcher	http://www.aignes.com/index.htm

Social Media Monitoring

Tool	Link
altervista	http://fb2rss.altervista.org
Feed Exileed	http://feed.exileed.com
Mention	https://en.mention.com
Queryfeed	http://www.queryfeed.net
Talkwalker	http://www.talkwalker.com
TwiSSR	http://www.twissr.com

Other Monitoring Tools

Tool	Link
InfoMinder	http://www.infominder.com/webminder
Keendly	http://keendly.com

Data Collation

Bookmarking

Tool	Link
Bibsonomy	http://www.bibsonomy.org
BonzoBox	http://bonzobox.com
Bookmark OS	https://bookmarkos.com
Booky	http://booky.io
ChannelKit	http://channelkit.com
Clipix	https://www.clipix.com
Curabase	https://www.curabase.com
Diigo	https://www.diigo.com
Dragdis	https://dragdis.com
Evernote	http://evernote.com
Dropmark	http://www.dropmark.com
eLink	https://elink.io
Email This	https://www.emailthis.me
FAVable	http://www.favable.com
Google Bookmarks	https://www.google.com/bookmarks
Granary	https://granary.pro
Historious	https://historio.us
Instapaper	http://www.instapaper.com
Juxtapost	http://www.juxtapost.com
Klart	https://klart.co

Larder	https://larder.io
Liner for Pocket	http://getliner.com/liner-for-pocket
Link.fish	https://link.fish
Linkman Pro	http://www.outertech.com/en/bookmarks-favorites
Linkstash	http://www.xrayz.co.uk
LiveBinders	http://www.livebinders.com
Lumio	https://www.lumioapp.com
memomize	http://www.memomize.com
Memonic	http://www.memonic.com
Microsoft OneNote	http://office.microsoft.com/en-us/onenote
mochimarks	https://mochimarks.com
netrostation	https://www.netrostation.com
P2K	https://p2k.co
Papaly	https://papaly.com
Paperwork	https://github.com/twostairs/paperwork
Pinboard	https://pinboard.in
Pearltrees	http://www.pearltrees.com
Pocket	http://getpocket.com
Raindrop	https://raindrop.io
Readibility	http://www.readability.com
Refind	https://refind.com
Save to Google	https://chrome.google.com/webstore/detail/save-to-google/meoeeoaohbmgbocpdpnjklmfmjjagkkf?utm_source=chrome-app-launcher-info-dialog
Scoop.it	http://www.scoop.it
Scrapbook	https://addons.mozilla.org/en-US/firefox/addon/scrapbook
Scrible	http://www.scrible.com
Session Buddy	https://chrome.google.com/webstore/detail/session-buddy/edacconmaakjimmfgnblocblbcdcpbko?hl=en
Sitehoover	http://www.sitehoover.com
Spaaze	http://www.spaaze.com
Stache	http://getstache.com
syncmarx	https://syncmarx.mcleodgaming.com

Thinkery	http://thinkery.me
Trackplanet	https://trackpanel.net
Trello	https://trello.com
Turtl	https://turtlapp.com
Tusk	https://github.com/klauscfhq/tusk
unhoard	https://www.unhoard.io
vookmark	https://vookmark.co
wallabag	https://wallabag.org
Wepware	http://www.wepware.com
Wonderpage	http://www.wonderpage.com
WorldBrain	https://worldbrain.io
Zotero	http://www.zotero.org

Notetaking

Tool	Link
Agenda	https://itunes.apple.com/us/app/agenda-a-new-take-on-notes/id1287445660
Bear Writer	http://www.bear-writer.com
Cherrytree	http://www.giuspen.com/cherrytree
Evernote	https://www.evernote.com
Google Keep	https://keep.google.com
Google Keep for Desktop	http://keepfordesk.xyz
inkdrop	https://www.inkdrop.info
Joplin	http://joplin.cozic.net
Kl1p	http://kl1p.com
Laverna	https://laverna.cc
Listacular	http://www.bloomingsoft.com/listacular
Microsoft OneNote	https://www.onenote.com
Milanote	http://www.milanote.com
Mindful	https://chrome.google.com/webstore/detail/mindful-beta/cieekmjjdkckhpidgaffphlaljdfhhab
Notebook	https://www.zoho.com/notebook
Outliney	https://glamdevelopment.com/outlinely/ios
Pear Note	http://www.usefulfruit.com/pearnote
Scribble	http://scribble.wreally.com
Simplenote	http://simplenote.com
Slite	https://slite.com
somnote	http://somcloud.com/about/somnote
Squid	http://squidnotes.com

Standard Notes	https://standardnotes.org
Thinkery	https://thinkery.me
Tomboy	https://wiki.gnome.org/Apps/Tomboy
Turtl	https://turtlapp.com
Tusk	https://github.com/klauscfhq/tusk
TypeLink	https://typelink.net
Workflowy	https://workflowy.com
wridea	http://wridea.com
Zoho Notebook	https://www.zoho.com/notebook

Annotation and Highlighting

Tool	Link
A.nnotate	http://a.nnotate.com
Beanote	https://chrome.google.com/webstore/detail/beanote-note-taking-on-we/nikccehomlnjkmgmhnieecolhgdafajb
Bounce	https://www.bounceapp.com
Diigo	https://www.diigo.com
Easy Annotate	http://www.easy-annotate.com
Highly	https://www.highly.co
Hypothesis	https://hypothes.is
Liner	http://getliner.com
Note Anywhere	https://chrome.google.com/webstore/detail/note-anywhere/bohahkiiknkelflnjjlipnaeapefmjbh
Pund.it	http://thepund.it
Skitch	https://evernote.com/skitch
Sum It Up	http://rachitgulati.com/sum-it-up
Weava Highlighter	https://chrome.google.com/webstore/detail/weava-highlighter-pdf-web/cbnaodkpfinfiipjblikofhlhlcickei

Screenshot and Screen Capture Tools

Tool	Link
1Click Screenshot	https://chrome.google.com/webstore/detail/1click-screenshot/akgpcdalpfphjmfifkmfbpdmgdmeeaeo?hl=en
Ashampoo Snap 9	https://www.ashampoo.com/en/usd/pin/1724/multimedia-software/Ashampoo-Snap-9
Awesome Screenshot	https://www.awesomescreenshot.com
BrowseShot	https://itunes.apple.com/us/app/browseshot/id615916400?ls=1%20&%20mt=12
Captur	http://cambhlumbulunk.blogspot.com/p/captur.html
Cockos LICEcap	https://www.cockos.com/licecap
EyeWitness	https://github.com/ChrisTruncer/EyeWitness
FastStone	http://www.faststone.org/FSCaptureDetail.htm
FireShot	https://getfireshot.com
Fraps	http://www.fraps.com
Full Page Screen Capture	https://chrome.google.com/webstore/detail/full-page-screen-capture/fdpohaocaechififmbbbbbknoalclacl?hl=en-US
Full Page Screenshot	https://chrome.google.com/webstore/detail/full-page-screenshot/glgomjpomoahpeekneidkinhcfjnnhmb?hl=en
Full Web Page Screenshots	https://addons.mozilla.org/en-US/firefox/addon/fireshot
Greenshot	https://getgreenshot.org
Gyazo	https://gyazo.com
jetScreenshot	http://www.jetscreenshot.com
Jing	https://www.techsmith.com/jing-tool.html
lazyshot	https://github.com/mdhama/lazyshot
LightShot	https://app.prntscr.com
Monosnap	https://monosnap.com

Nimbus	http://nimbus.everhelper.me
Pages 2 Images	http://www.page2images.com
Paparazzi!	https://derailer.org/paparazzi
PickPick	http://ngwin.com/picpick
puush	https://puush.me
qSnap	https://chrome.google.com/webstore/detail/qsnap-screen-capture-scre/bijakfpegjnjmfdoiloebhaemhomjkon
Screengrab	https://addons.mozilla.org/en-US/firefox/addon/screengrab-fix-version/
Screen Master	https://play.google.com/store/apps/details?id=pro.capture.screenshot
Screenshot App	http://screenshotapp.com
Screenshot Captor	http://www.donationcoder.com/software/mouser/popular-apps/screenshot-captor
Screenshot Layer	https://screenshotlayer.com
Screenshot Machine	https://www.screenshotmachine.com
Screenshot Utility	http://screenshot-utility.com
ScreenToGif	http://www.screentogif.com
ShareX	https://getsharex.com
Shrink the Web	https://www.shrinktheweb.com
SiteShoter	http://www.nirsoft.net/utils/web_site_screenshot.html
Snaggy	https://snag.gy
Snagit	https://www.techsmith.com/screen-capture.html
Snapito	https://snapito.com
Snapper	https://github.com/dxa4481/Snapper
Snip&Paste	https://www.snipaste.com
Take Webpage Screenshots Entirerly	https://chrome.google.com/webstore/detail/take-webpage-screenshots/mcbpblocgmgfnpjjppndjkmgjaogfceg?hl=en-US
TinyTake	https://tinytake.com
URL2PNG	https://www.url2png.com
URL Box	https://urlbox.io
Web-Capture	https://web-capture.net
Web Page Saver	https://www.magnetforensics.com/free-tool-web-page-saver
webscreenshot	https://github.com/maaaaz/webscreenshot

Browsing and Browsers

Browsers

Tool	Link
Addap's	https://www.addaps.com
Alloy	http://alloy.simoncaminada.ch
Aloha Browser	https://alohabrowser.com
Basilisk	http://www.basilisk-browser.org
Brave	https://brave.com
CentBrowser	http://www.centbrowser.com
Chrome	https://www.google.com/chrome
Chromium	https://www.chromium.org
Cliqz	https://cliqz.com
Colibri	https://colibri.opqr.co
Comodo Dragon	https://www.comodo.com/home/browsers-toolbars/browser.php
Cocoon	https://getcocoon.com
Coowon	http://coowon.com
Dooble	https://textbrowser.github.io/dooble
Edge	https://www.microsoft.com/en-us/windows/microsoft-edge/microsoft-edge
Firefox	https://www.mozilla.org
Ghost Browser	https://ghostbrowser.com
Iridium	https://iridiumbrowser.de
Konqueror	https://konqueror.org
Links	http://links.twibright.com

Maxthon	http://www.maxthon.com
Midori	http://midori-browser.org
Min	https://minbrowser.github.io/min
Next	http://next-browser.com
Opera	http://www.opera.com
Opera Neon	http://www.opera.com/computer/neon
Pale Moon	https://www.palemoon.org
Qt Web	http://www.qtweb.net
QupZilla	https://www.qupzilla.com
Safari	http://www.apple.com/safari
SeaMonkey	https://www.seamonkey-project.org
Silo	https://www.authentic8.com/overview
Sleipnir	http://www.fenrir-inc.com/jp/sleipnir
SRWare Iron	http://www.srware.net/en/software_srware_iron.php
Torch	http://www.torchbrowser.com
UCBrowser	http://www.ucweb.com
Vivaldi	https://vivaldi.com
Yandex Browser	https://browser.yandex.com/desktop/main

Startpages

Tool	Link
allmyfaves	http://www.allmyfaves.com
ighome	http://www.ighome.com
iloggo	http://iloggo.com
Kadaza	http://www.kadaza.com
Myfav.es	http://myfav.es
My Yahoo	https://my.yahoo.com
Open OOX	https://openoox.com
Protopage	http://www.protopage.com
Start.io	http://start.io
Startme	http://www.startme.com
Symbaloo	http://www.symbaloo.com
uStart.org	http://www.ustart.org
Yourport	http://www.yourport.com
Zenstart	http://www.zenstart.com

Customising New Tab

Tool	Link
Blink	https://addons.mozilla.org/en-GB/firefox/addon/blink
Bookmark Dial	https://addons.mozilla.org/en-GB/firefox/addon/bookmark-dial
Chrome Customize Your New Tab Page	https://chrome.google.com/webstore/category/collection/customize_your_new_tab_page
Custom New Tabs	https://addons.mozilla.org/en-US/firefox/addon/custom-new-tabs
Live Start Page LST	https://addons.mozilla.org/en-US/firefox/addon/live-start-page-lst
Moment	https://addons.mozilla.org/en-US/firefox/addon/moment/?src=search
New MetroTab	https://addons.mozilla.org/en-US/firefox/addon/new-metrotab
New Tab Tools	https://addons.mozilla.org/en-US/firefox/addon/new-tab-tools
Rocket Dashboard	https://chrome.google.com/webstore/detail/rocket-dashboard/plcedaomjjdiihihamfhangiiknamifc?utm_source=website&utm_medium=splash&utm_campaign=temp-splash
SiteLauncher	https://addons.mozilla.org/en-GB/firefox/addon/sitelauncher
Speed Dial New Tab Page	https://addons.mozilla.org/en-US/firefox/addon/fvd-speed-dial
Speed Start	https://addons.mozilla.org/en-GB/firefox/addon/speed-start
Start.me	https://addons.mozilla.org/en-US/firefox/addon/startme
Super Start	https://addons.mozilla.org/en-GB/firefox/addon/super-start

ViewMarks	https://addons.mozilla.org/en-US/firefox/addon/viewmarks

Tab Management

Tool	Link
Bookmark Ninja	https://www.bookmarkninja.com
OneTab	https://chrome.google.com/webstore/detail/onetab/chphlpgkkbolifaimnlloiipkdnihall?hl=en
MySessions	https://addons.mozilla.org/en-US/firefox/addon/my-sessions
Quick Tab	https://chrome.google.com/webstore/detail/quick-tab/bdeifmcaonlafkglbdpbbhkeecjnkipo
Session Buddy	https://chrome.google.com/webstore/detail/session-buddy/edacconmaakjimmfgnblocblbcdcpbko?hl=en
Tabli	https://chrome.google.com/webstore/detail/tabli/igeehkedfibbnhbfponhjjplpkeomghi
TabCloud	https://chrome.google.com/webstore/detail/tabcloud/npecfdijgoblfcgagoijgmgejmcpnhof?hl=en
Tab Hibernation	https://chrome.google.com/webstore/detail/tab-hibernation/pbdpajcdgknpendpmecafmopknefafha?hl=en
TabJump	https://chrome.google.com/webstore/detail/tabjump-intelligent-tab-n/hokofmgcicpnjchllaccgedmmmbbnbmf?hl=en
Tab Manager	https://addons.mozilla.org/en-US/firefox/addon/tab-manager-webextension
Tab Manager	https://addons.mozilla.org/en-US/firefox/addon/tab_manager
Tabs Outliner	https://chrome.google.com/webstore/detail/tabs-outliner/eggkanocgddhmamlbiijnphhppkpkmkl
TabsPlus	https://chrome.google.com/webstore/detail/tabsplus/nikomkkhhpfoeamojhhgpfkpkdlfhfii?hl=en

Tab Session Manager	https://addons.mozilla.org/en-US/firefox/addon/tab-session-manager
Tab Wrangler	https://chrome.google.com/webstore/detail/tab-wrangler/egnjhciaieeiiohknchakcodbpgjnchh?hl=en
The Great Suspender	https://chrome.google.com/webstore/detail/the-great-suspender/klbibkeccnjlkjkiokjodocebajanakg
Toby	https://www.gettoby.com
TooManyTabs	https://chrome.google.com/webstore/detail/toomanytabs-for-chrome/amigcgbheognjmfkaieeeadojiibgbdp?hl=en

Extension Managers

Tool	Link
Addons Manager Hilite	https://addons.mozilla.org/en-US/firefox/addon/addons-manager-hilite/?src=search
Add-ons Manager Context Menu	https://addons.mozilla.org/en-US/firefox/addon/am-context
Custom Chrome	https://chrome.google.com/webstore/detail/custom-chrome-extension-m/balnpimdnhfiodmodckhkgneejophhhm
Extensions Manager (aka Switcher)	https://chrome.google.com/webstore/detail/extensions-manager-aka-sw/lpleipinonnoibneeejgjnoeekmbopbc?hl=en
Extension Manager Extended	https://addons.mozilla.org/en-US/firefox/addon/extension-manager-extended
Extensity	https://chrome.google.com/webstore/detail/extensity/jjmflmamgggndanpgfnpelongoepncg/reviews
My Extensions	https://chrome.google.com/webstore/detail/my-extensions/igejgfmbjjjjplnnlgnbejpkpdajkblm?hl=en
One Click Extensions Manager	https://chrome.google.com/webstore/detail/one-click-extensions-mana/pbgjpgbpljobkekbhnnmlikbbfhbhmem?hl=en
Simple Add-on Manager	https://addons.mozilla.org/en-US/firefox/addon/simple-add-on-manager

Offline Browsing

Tool	Link
A1 Website Download	http://www.microsystools.com/products/website-download
Cyotek WebCopy	http://www.cyotek.com/cyotek-webcopy
gmapcatcher	https://github.com/heldersepu/gmapcatcher
Hooey webprint	http://www.hooeeywebprint.com.s3-website-us-east-1.amazonaws.com/download.html
HTTrack	http://www.httrack.com
Offliberty	http://offliberty.com
Resolver	https://metaproductsrevolver.com
ScrapBook	https://addons.mozilla.org/en-US/firefox/addon/scrapbook
SiteSucker	http://ricks-apps.com/osx/sitesucker/index.html
WebAssistant	http://www.proxy-offline-browser.com/download.html
Website Ripper Copier	http://www.tensons.com/products/websiterippercopier

Browsing History

Tool	Link
Chrome History View	https://www.nirsoft.net/utils/chrome_history_view.html
Falcon	https://chrome.google.com/webstore/detail/falcon/mmifbbohghecjloeklpbinkjpbplfalb?hl=en
Fea KeyLogger	https://chrome.google.com/webstore/detail/fea-keylogger/fgkghpghjcbfcflhoklkcincndlpobja?hl=en
Fiddler	https://www.telerik.com/download/fiddler
History Search	https://historysearch.com
Hunchly	https://www.hunch.ly

Other Browsing Tools

Tool	Link
AutoPagerize	https://chrome.google.com/webstore/detail/autopagerize/igiofjhpmpihnifddepnpngfjhkfenbp
Block Facebook	https://sarimhaq.github.io/block-facebook-website
Downforeveryoneorjustme	http://downforeveryoneorjustme.com
Finitimus	https://chrome.google.com/webstore/detail/finitimus/ckdjcgaagfcnndkknfmncedapdjaokb?utm_source=chrome-ntp-icon
Google When	https://chrome.google.com/webstore/detail/google-when/dgafcidlgmbcehokgdeghmfnbpbfhihh
Panic Button	https://chrome.google.com/webstore/detail/panicbutton/faminaibgiklngmfpfbhmokfmnglamcm
Pawblock	https://www.pawblock.dannyguo.com
Referer Control	https://chrome.google.com/webstore/detail/referer-control/hnkcfpcejkafcihlgbojoidoihckciin?hl=en
SelfControl	http://selfcontrolapp.com
Simple Blocker	https://chrome.google.com/webstore/detail/simple-blocker/akfbkbiialncppkngofjpglbbobjoeoe
User-Agent Switcher for Chrome	https://chrome.google.com/webstore/detail/user-agent-switcher-for-c/djflhoibgkdhkhhcedjiklpkjnoahfmg

Writing and Dissemination

Writing and Office Tools

Tool	Link
Arguman	http://en.arguman.org
bibisco	http://www.bibisco.com
Bibme	http://www.bibme.org
Cite This For Me	https://chrome.google.com/webstore/detail/cite-this-for-me-web-cite/nnnmhgkokpalnmbeighfomegjfkklkle?hl=en
Citationsy	https://citationsy.com
Classeur.io	http://classeur.io
CustomWritings.com: Citation Generator	https://www.customwritings.com/citation_generator.html
FreeOffice	http://www.freeoffice.com
Grammarly	https://chrome.google.com/webstore/detail/grammarly-for-chrome/kbfnbcaeplbcioakkpcpgfkobkghlhen?hl=en
GoogleDocs	https://www.google.com/docs/about
Hemmingway Editor	http://hemingwayapp.com
KingSoft	http://www.kingsoftstore.com
LibreOffice	https://www.libreoffice.org
Manuskript	http://www.theologeek.ch/manuskript
MS Office	https://products.office.com
Office Online	https://chrome.google.com/webstore/detail/office-online/ndjpnladcallmjemlbaebfadecfhkepb/related
Ommwriter	https://ommwriter.com
OmniOutliner	https://www.omnigroup.com/omnioutliner
OnlyOffice	https://www.onlyoffice.com

oStoryBook	http://ostorybook.tuxfamily.org
oTranscribe	http://otranscribe.com
Plume Creator	http://plume-creator.eu
Scrivener	http://literatureandlatte.com/scrivener.php
StoryToolz	http://storytoolz.com
TextExpander	https://smilesoftware.com/textexpander
UltraEdit	http://www.ultraedit.com
Ulysses	https://ulyssesapp.com
wordnik	http://wordnik.com
WriteApp	https://writeapp.me
Write or Die	http://writeordie.com
Writer's Cafe	http://www.writerscafe.co.uk

Slideshow and Presentation Tools

Tool	Link
Canva	https://www.canva.com/create/presentations
Deckset	http://www.decksetapp.com
emaze	https://www.emaze.com
FlowVella	https://flowvella.com
genially	https://www.genial.ly
GoogleDocs	https://docs.google.com
Haiku Deck	https://www.haikudeck.com
Keynote	http://www.apple.com/de/mac/keynote
KingSoft	http://ksosoft.com/product/presentation-free.html
KnowledgeVision	http://www.knowledgevision.com
LibreOffice	https://www.libreoffice.org
Live Slides	https://www.liveslides.com
Mighty Meeting	http://www.mightymeeting.com
MS Office	https://products.office.com
Paste	https://fiftythree.com/paste
Piktochart	https://piktochart.com
Pitch Deck	https://pitchdeck.io
Powtoon	https://www.powtoon.com
presenterswall	http://www.presenterswall.com
Prezent 3D	https://www.prezent3d.com
Prezi	https://prezi.com
Slidebean	https://slidebean.com
Slidedog	http://slidedog.com
SlidePresenter	http://www.slidepresenter.com

SlideRocket	https://www.clearslide.com/product/sliderocket
Slides	https://slides.com
SpeechInMinutes	http://www.speechinminutes.com/
Sway	https://sway.com
WebSlides	https://webslides.tv
vcasmo	http://www.vcasmo.com
Visme	http://www.visme.co
Zoho Docs	https://www.zoho.com/docs/show.html

Digital Publishing

Tool	Link
Canva	https://www.canva.com
Doclayer	https://standaert.net/doclayer
Issuu	https://issuu.com
Lucidpress	https://www.lucidpress.com
Mag.io	http://mag.io
My eBook	http://www.myebook.com
Omeka	http://omeka.org
Scribd	https://www.scribd.com
Yudu	http://yudu.com

Newsletter Tools

Tool	Link
AWeber	http://www.aweber.com
BombBomb	http://bombbomb.com
Campayn	http://campayn.com
Canva	https://www.canva.com
ConstantContact	http://www.constantcontact.com
Freshmail	http://freshmail.com
GetResponse	http://www.getresponse.com
iContact	https://www.icontact.com
MadMimi	https://madmimi.com
Mailchimp	http://mailchimp.com
Mailjet	https://www.mailjet.com
Mailup	http://www.mailup.com
Newsletter Creator for Gmail	https://chrome.google.com/webstore/detail/newsletter-creator-for-gm/cihaednhfbocfdiflmpccekcmjepcnmb
sendinblue	https://www.sendinblue.com
Sendicate	https://www.sendicate.net
Sendloop	https://sendloop.com
Signupto	https://www.signupto.com
TinyLetter	http://tinyletter.com
VerticalResponse	http://www.verticalresponse.com
Vision6	http://www.vision6.com.au

Digital Storytelling

Tool	Link
Adobe Spark	https://spark.adobe.com/
Animatron	https://www.animatron.com
Animoto	https://animoto.com
Atavist	https://atavist.com
Closr	https://www.closr.it
Eko Studio	https://studio.helloeko.com
Juxtapose	https://juxtapose.knightlab.com
Klynt	http://www.klynt.net
MakeBeliefsComix	http://www.makebeliefscomix.com
Metta	http://www.metta.io
Neatline	http://neatline.org
Odyssey	https://cartodb.github.io/odyssey.js
Pageflow	http://pageflow.io
Photodex	http://www.photodex.com
Piclits	http://www.piclits.com/compose_dragdrop.aspx
Racontr	https://racontr.com
RaptMedia	http://www.raptmedia.com
RawShorts	http://www.rawshorts.com
Shorthand Social	https://shorthand.com/social
Soundcite	http://soundcite.knightlab.com
sStory	https://ejfox.github.io/sStory
Steller	https://steller.co
Storify	https://storify.com
Storyboard	http://generator.acmi.net.au/storyboard

Storyform	https://storyform.co
StoryMap	https://storymap.knightlab.com
StoryMaps	http://storymaps.arcgis.com
Sway	https://sway.com
Thinglink	https://www.thinglink.com
Timeline	http://timeline.knightlab.com
Tripline	http://www.tripline.net
Visual Investigative Scenarios	https://vis.occrp.org
Wevideo	https://www.wevideo.com
VideoScribe	http://www.videoscribe.co

Wikis, Websites, and Web Apps

Wikis

Tool	Link
DokuWiki	https://www.dokuwiki.org/dokuwiki
Foswiki	http://foswiki.org
Matterwiki	http://matterwiki.com
MediaWiki	https://www.mediawiki.org/wiki/MediaWiki
Nuclino	https://www.nuclino.com
PmWiki	http://www.pmwiki.org
Scribbleton	http://scribbleton.com
TiddlyWiki	http://tiddlywiki.com
Tiki Wiki	https://info.tiki.org
Torchpad	https://torchpad.com
TWiki	http://twiki.org
Wikia	http://www.wikia.com/Wikia
Wikidot	http://www.wikidot.com
Wikispaces	http://www.wikispaces.com
wikidPad	http://wikidpad.sourceforge.net
Zim	http://zim-wiki.org/downloads.html

Website Builders

Tool	Link
Boldgrid	https://www.boldgrid.com
Duda	https://www.duda.co
eHost	https://www.ehost.com
GoDaddy	https://ca.godaddy.com/websites/website-builder
Google Sites	https://gsuite.google.com/products/sites
IM Creator	http://www.imcreator.com
jimdo	https://www.jimdo.com
LonelyPage	http://www.lonelypage.io
Publishthis.email	https://www.publishthis.email
Sheet2site	https://www.sheet2site.com
Simvoly	https://simvoly.com
Site Builder	https://www.sitebuilder.com
Sitey	https://www.sitey.com
Squarespace	https://www.squarespace.com
Strikingly	https://www.strikingly.com
UCoz	https://www.ucoz.com
UCraft	https://www.ucraft.com
Ukit	https://ukit.com
Voog	https://www.voog.com
Web.com	https://www.web.com
Webnode	https://us.webnode.com
Website Builder	https://www.websitebuilder.com
Webstarts	https://www.webstarts.com
Weebly	https://www.weebly.com

Wix	https://www.wix.com
Wordpress	https://wordpress.com
yola	https://www.yola.com
Zoho	https://www.zoho.com/sites/website-builder.html

App Builders

Tool	Link
Appery.io	https://appery.io
AppsBar	http://www.appsbar.com
AppsBuilder	http://www.apps-builder.com
Apps Geyser	https://www.appsgeyser.com
App Machine	http://www.appmachine.com
AppMakr	http://www.appmakr.com
Appy Pie	https://www.appypie.com
bubble	https://bubble.is
Build Fire	https://buildfire.com
Bizness Apps	https://www.biznessapps.com
ChupaMobile	https://www.chupamobile.com
Game Salad	https://gamesalad.com
Good Barber	https://www.goodbarber.com/native
iBuild App	https://ibuildapp.com
Kony	https://www.kony.com/products/appplatform#download?utm_medium=tpp&utm_source=businessofapps&utm_campaign=19q1-pf-business-of-apps&utm_content=notapp&utm_term=notapp&utm_adgroup=notapp&kash=notapp
Mobile Roadie	https://mobileroadie.com
Shoutem	http://www.shoutem.com
The App Builder	https://www.theappbuilder.com

Mind Mapping, Concept Mapping and Idea Generation

Mind Mapping, Concept Mapping and Idea Generation Tools

Tool	Link
The Brain	http://www.thebrain.com
Bubbl.us	https://bubbl.us
Cmap	https://cmap.ihmc.us
Comapping	http://www.comapping.com
ConceptDraw	http://www.conceptdraw.com
Coogle	https://coggle.it
DebateGraph	https://debategraph.org
Fast Idea Generator	http://diytoolkit.org/tools/fast-idea-generator-2
Freemind	http://freemind.sourceforge.net/wiki/index.php/Main_Page
Freeplane	http://freeplane.sourceforge.net/wiki/index.php/Main_Page
Germ	https://germ.io
GroupMap	http://www.groupmap.com
Ideaphora	http://www.ideaphora.com
iMindMap	https://imindmap.com
iMindQ	https://www.imindq.com
Lucidchart	https://www.lucidchart.com
Mattermap	https://www.mattermap.nl
Mind42	http://mind42.com
Mind Genius	http://www.mindgenius.com
Mindjet	https://www.mindjet.com

Mind Map	https://chrome.google.com/webstore/detail/mindmap/gdaeohpmcenmffofpikllphdhlkkocfa#detail/mindmap/gdaeohpmcenmffofpikllphdhlkkocfa
Mind Mup	https://www.mindmup.com
Mindmeister	https://www.mindmeister.com
Mindomo	https://www.mindomo.com
Org-brain	https://github.com/Kungsgeten/org-brain
Popplet	http://popplet.com
Realtimeboard	https://realtimeboard.com
Scapple	http://literatureandlatte.com/scapple.php
Simple Mind	https://simplemind.eu
Sketchboard	http://sketchboard.io
Slatebox	https://slatebox.com
Spiderscribe	http://www.spiderscribe.net
Stormboard	https://stormboard.com
Text2MindMap	https://tobloef.com/text2mindmap
VUE	http://vue.tufts.edu
Wise Maping	http://www.wisemapping.com
yWorks	http://www.yworks.com/en/products_yed_gallery.html
Xmind	http://www.xmind.net

Productivity and File Management

Main Work Management and Productivity Tools

Tool	Link
2Do	http://www.2doapp.com
Any.do	http://www.any.do
Asana	https://asana.com
Boomerang App	http://www.boomerangapp.com
Dapulse	https://dapulse.com
Dayboard	https://dayboard.co
Droptask	https://www.droptask.com
Flask	http://flask.io
Focus booster	https://www.focusboosterapp.com
Freecamp	https://freedcamp.com
Leechblock	https://addons.mozilla.org/en-US/firefox/addon/leechblock
minimalist	http://www.getminimalist.com
MorningRoutine	http://www.ubicolor.com/morningroutine.html
MyLifeOrganized	http://www.mylifeorganized.net
Noteplan	https://noteplan.co
Pintask	https://pintask.me
PomodoroTechnique	http://pomodorotechnique.com
Producteev	https://www.producteev.com
Quire	https://quire.io
Remember the Milk	https://www.rememberthemilk.com
RescueTime	https://www.rescuetime.com
Restya	http://restya.com

StayFocusd	https://chrome.google.com/webstore/detail/stayfocusd/laankejkbhbdhmipfmgcngdelahlfoji/details
Taskboard	https://taskboard.matthewross.me
TikiTiki	https://ticktick.com
Tinygain	https://tinygain.com
Trello	https://trello.com
Todo.ly	https://todo.ly
Todo	http://todotxt.com
Todoist	https://en.todoist.com
Toggl	https://www.toggl.com
Tomighty	http://www.tomighty.org
Toodledo	https://www.toodledo.com
Workflowy	https://workflowy.com
Wunderlist	https://www.wunderlist.com

Calendars and Scheduling

Tool	Link
Assistant	http://www.assistant.to
Bunchapp	http://bunchapp.io
Calendly	https://calendly.com
Cozi	http://www.cozi.com
Doodle	http://doodle.com
Foogi	http://www.foogi.me
Fruux	https://fruux.com
Meekan	https://meekan.com
Meetin.gs	http://www.meetin.gs
MyMemorizer	http://www.mymemorizer.com
Noteplan	https://noteplan.co
ScheduleOnce	http://www.scheduleonce.com
TeamUp	http://www.teamup.com
Teamweek	https://teamweek.com

E-mail Management

Tool	Link
ActiveInbox	http://www.activeinboxhq.com
Batched Inbox	https://www.batchedinbox.com
Baydin	https://www.baydin.com
BetterGmail	https://addons.mozilla.org/en-US/firefox/addon/better-gmail-2/
Block Sender	https://chrome.google.com/webstore/detail/block-sender/bklnjbfcmglhiaoppcckdodanccbelcg
Boomerang Mail	http://www.boomeranggmail.com
ClearContext	http://www.clearcontext.com
Cleanfox	https://www.cleanfox.io
Complete	https://complete.li
FindBigMail	https://www.findbigmail.com
Followupthen	https://www.followupthen.com
gpum	https://addons.mozilla.org/en-US/firefox/addon/gpum
Hiver	http://hiverhq.com
Integrated gmail	https://addons.mozilla.org/en-US/firefox/addon/integrated-gmail
Mailstore	http://www.mailstore.com
Hubspotsales	https://chrome.google.com/webstore/detail/hubspot-sales/oiiaigjnkhngdbnoookogelabohpglmd?hl=en
Minimalist	https://chrome.google.com/webstore/detail/minimalist-for-everything/bmihblnpomgpjkfddepdpdafhhepdbek
NudgeMail	https://www.nudgemail.com
Rapportive	https://rapportive.com
Sanebox	https://www.sanebox.com
Send for Gmail	https://chrome.google.com/webstore/detail/send-from-gmail-by-google/pgphcomnlaojlmmcjmiddhdapjpbgeoc

Sortd	http://www.sortd.com
TrueNew	https://chrome.google.com/webstore/detail/truenewtm-count-for-gmail/lhgbgmbdabgjdephnmkpmcdkmnpiahlb
Ugly Email	https://uglyemail.com
Unroll.me	https://unroll.me
WiseStamp	https://chrome.google.com/webstore/detail/wisestamp-email-signature/pbcgnkmbeodkmiijjfnliicelkjfcldg

Cloud Storage and File Sharing

Tool	Link
4Shared	http://www.4shared.com
ADrive	http://www.adrive.com
Amazon Cloud drive	https://www.amazon.com/clouddrive/home
Box	https://www.box.com
Boxcryptor	https://www.boxcryptor.com
Cloudapp	http://www.getcloudapp.com
CloudFuze	https://www.cloudfuze.com
CloudHQ	https://www.cloudhq.net
docuvo	https://www.docuvo.com
Dropbox	https://www.dropbox.com
Dropcanvas	http://dropcanvas.com
droplr	https://droplr.com
DropSend	http://www.dropsend.com
Duplicati	http://www.duplicati.com
Egnyte	http://www.egnyte.com
EnCrypted Cloud	https://www.encryptedcloud.com
Ge.TT	http://ge.tt
GoodSync	http://www.goodsync.com
Google Drive	https://www.google.com/intl/nl/drive
Hightail	https://www.hightail.com
hubiC	https://hubic.com
iCloud	https://www.icloud.com
Mediafire	https://www.mediafire.com
Mega	https://mega.nz

Mindbox	https://minbox.com
Mozy	http://mozy.com
Multicloud	https://www.multcloud.com
Onedrive	https://onedrive.live.com
Onehub	https://www.onehub.com
Otixo	http://www.otixo.com
pCloud	https://www.pcloud.com
Sendthisfile	https://www.sendthisfile.com
Sendspace	https://www.sendspace.com
Simple.Savr	https://www.ssavr.com
Spideroak	https://spideroak.com
SugarSync	https://www.sugarsync.com
Syncthing	https://syncthing.net
TransferBigFiles	https://www.transferbigfiles.com
Tresorit	https://tresorit.com
WeTransfer	https://www.wetransfer.com

Web Automation

Tool	Link
Apiant	https://apiant.com
Cloud Work	https://cloudwork.com
IFTTT	https://ifttt.com
Microsoft Flow	https://flow.microsoft.com
Stringify	https://www.stringify.com
Trigger Happy	https://trigger-happy.eu
WeWiredWeb	https://wewiredweb.com
Workflow	https://workflow.is
Zapier	https://zapier.com

Collaboration and Communication

Collaboration and Project Management

Tool	Link
10kinsights	https://www.10000ft.com
92fiveApp	http://92fiveapp.com
5pm	http://www.5pmweb.com
ActionMint	https://www.actionmint.com
ActiveCollab	https://www.activecollab.com
Advanseez	http://www.advanseez.com
Agilewords	http://www.agilewords.com
Airtable	https://airtable.com
AllThings	http://www.allthings.io
Any.do	http://www.any.do
Apollo	http://www.apollohq.com
Asana	https://asana.com
Authorea	https://www.authorea.com
AWW	https://awwapp.com
Azendoo	https://www.azendoo.com
Basecamp	https://basecamp.com
Binfire	https://www.binfire.com
Box	https://www.box.com
Breeze	https://www.breeze.pm
Canvanizer	https://canvanizer.com
Casual	https://casual.pm

Cardboardit	https://cardboardit.com
Cardsmith	http://cardsmith.co
CloudApp	http://www.getcloudapp.com
Collabtive	http://collabtive.o-dyn.de
CollaborateCloud	http://www.collaboratecloud.com
Comindwork	http://www.comindwork.com
Conceptboard	https://conceptboard.com
Confluence	https://www.atlassian.com/software/confluence
CoSketch	http://cosketch.com
Crowdbase	http://crowdbase.com
Deekit	https://www.deekit.com
Draw.to	http://draw.to
eGroupWare	http://www.egroupware.org
Elegantt	https://elegantt.com
Encrypted Cloud	https://www.encryptedcloud.com
Firepad	https://firepad.io
Firesub	https://firesub.com
Flask	http://flask.io
Float	https://www.float.com
Flowdock	https://www.flowdock.com
Flockdraw	http://flockdraw.com
Flow	https://www.getflow.com
Frame	https://frame.io
Freedcamp	https://freedcamp.com
Glasscubes	https://www.glasscubes.com
GQueues	https://www.gqueues.com
Hightail	https://www.hightail.com
hitask	https://hitask.com
Huddle	https://www.huddle.com
Idea Flip	https://ideaflip.com
Infolio	https://infolio.co
KabanTool	http://kanbantool.com
Kanboard	https://kanboard.net

Kerika	http://kerika.com
Loomio	https://www.loomio.org
LumoFlow	https://lumoflow.com
Nozbe	https://nozbe.com
Nutcache	http://www.nutcache.com
meistertask	https://www.meistertask.com
Minute	https://www.getminute.com
Monday	https://monday.com
Mural	https://mural.co
MyKanzen	https://mykanzen.com
OmniGroup	https://www.omnigroup.com
OnlyOffice	https://www.onlyoffice.com
Padlet	https://padlet.com
Piematrix	http://www.piematrix.com
Pinstriped	http://pinstriped.com
PivotalTracker	http://www.pivotaltracker.com
Plan	https://plan.io
Planleaf	http://www.planleaf.com
Planzone	https://www.planzone.com
Podio	https://podio.com
PrimaryPad	http://primarypad.com
ProjectManager	https://www.projectmanager.com
ProjectPlace	https://www.projectplace.com
ProofHub	https://www.proofhub.com
Quip	https://quip.com
Quire	https://quire.io
Realtimeboard	https://realtimeboard.com
Redbooth	https://redbooth.com
Reverb	http://reverbapp.com
ScadaPlan	http://scadaplan.com
SeavusProjectViewer	https://www.seavusprojectviewer.com
Smartsheet	https://www.smartsheet.com
Stackfield	https://www.stackfield.com

Stormboard	https://www.stormboard.com
SyncSpace	http://infinitekind.com/syncspace
Taiga	https://taiga.io
Taskboard	https://taskboard.matthewross.me
táve	https://tave.com
TeamAllocator	http://www.teamallocator.com
Team.fm	https://team.fm
Team Pad	https://www.team-pad.com
TeamWork	https://www.teamwork.com
TeamWorklive	http://www.teamworklive.com
Transparent Business	http://transparentbusiness.com
Trello	https://trello.com
Tuzzit	https://www.tuzzit.com
Twiddla	http://www.twiddla.com
Twoodo	https://www.twoodo.com
updatey	http://updatey.com
Web Whiteboard	http://webwhiteboard.com
Weekdone	https://weekdone.com
wePaste	http://www.wepaste.com
Whiteboard	http://whiteboard.drewwilson.com
Whiteboard Fox	https://whiteboardfox.com
Workfront	https://www.workfront.com
Wrike	https://www.wrike.com
Yammer	https://www.yammer.com
YouTrack	https://www.jetbrains.com/youtrack
Zoho	https://www.zoho.com

Communication Tools

Tool	Link
Adobe Connect	http://www.adobe.com/products/adobeconnect.html
AnyDesk	http://anydesk.com/remote-desktop
AnyMeeting	https://www.anymeeting.com
Auralink	http://auralink.com
Babblebay	http://www.babblebay.com
BeamYourScreen	http://www.beamyourscreen.com
Blackboard	http://www.blackboard.com/online-collaborative-learning/index.aspx
blind	https://us.teamblind.com
Briar	https://briarproject.org
Cisco Spark	https://notes.ciscospark.com
clearvale	https://www.clearvale.com/marketing/en
Digital Samba	http://www.digitalsamba.com
Discourse	http://www.discourse.org
eBLVD	https://www.eblvd.com
Ekiga	http://ekiga.org
FaceFlow	http://www.faceflow.com
Fleep	https://fleep.io
FreeConferenceCall	https://www.freeconferencecall.com
FreeScreenSharing	https://www.freescreensharing.com
Friends	http://moose-team.github.io/friends
Glance	http://ww2.glance.net
GoToMeeting	http://www.gotomeeting.com
Highfive	https://highfive.com

icq	https://icq.com
iLinc	http://www.ilinc.com
Infinite	http://www.infiniteconferencing.com
Intercall	http://www.intercall.com
Jitsi	https://jitsi.org
Join.me	https://www.join.me
Jostle	http://www.jostle.me
KIK	https://www.kik.com
Let's Chat	http://sdelements.github.io/lets-chat
lifesize	http://www.lifesize.com
Line	https://line.me
Linphone	http://www.linphone.org
Live Conference Pro	http://www.liveconferencepro.com
Lucid Meetings	http://www.lucidmeetings.com
Meet Franz	https://meetfranz.com
MeetingOne	https://www.meetingone.com
MeetNotes	https://meetnotes.co
MeWe	https://mewe.com
mikogo	https://www.mikogo.com
mobilimeet	http://mobilimeet.com
MyBB	http://www.mybb.com
PGi iMeet	http://www.pgi.com/imeet
Phorum	http://www.phorum.org
Quicktopic	http://www.quicktopic.com
ReadyTalk	https://www.readytalk.com
RingCentral	http://www.ringcentral.com
Rocket.Chat	https://rocket.chat
screenleap	http://www.screenleap.com
sifonr	http://www.sifonr.com/
Signal	https://signal.org
Skype	http://www.skype.com
Slack	https://slack.com
StartMeeting	https://www.startmeeting.com

Stride	https://www.stride.com
Talky	https://talky.io
Teamviewer	https://www.teamviewer.com
Telegram	https://telegram.org
Tibbr	http://www.tibbr.com
Tixeo	https://www.tixeo.com/en/secure-video-conferencing
Toc	http://toc.im
TrueConf	http://trueconf.com
Twchat	http://twchat.com
Vanilla Forums	http://vanillaforums.org
Veeting rooms	https://www.veeting.com
VeriShow	http://www.verishow.com
Viadesk	http://www.viadesk.com
VideoLink2	https://videolink2.me
Webex	http://www.webex.com
Webinato	http://www.webinato.com
WeChat	https://web.wechat.com
WhatsApp	https://www.whatsapp.com
Zeetings	http://www.zeetings.com
Zoho Meeting	https://www.zoho.com/meeting
Zoom.us	https://zoom.us
Zulip	https://www.zulip.org

Other Utility Tools

File Converters

Tool	Link
Adapter	https://macroplant.com/adapter
Any Video Converter	http://www.any-video-converter.com/products/for_video_free
Apowersoft	https://www.apowersoft.com/free-online-video-converter
Avidemux	http://avidemux.sourceforge.net
Batch Photo	https://www.batchphoto.com/espresso
cloudconvert	https://cloudconvert.com
Clip Convert	https://clipchamp.com/en/video-converter
Cometdocs	https://www.cometdocs.com
Convert Files	http://www.convertfiles.com
Convert Video Online	https://convert-video-online.com
CoolUtils	https://www.coolutils.com/online/Image-Converter
Covertion	https://convertio.co
DVD Video Soft	https://www.dvdvideosoft.com/products/dvd/Free-Image-Convert-and-Resize.htm
Fileshifter	https://fileshifter.io
File Zig Zag	https://www.filezigzag.com
Free File Convert	https://www.freefileconvert.com
Free Make	http://www.freemake.com/free_video_converter
NCH Software	https://www.nchsoftware.com/software/converters.html
Online-Convert	https://www.online-convert.com

PDF Converter	https://www.freepdfconvert.com
PDF Converter	https://smallpdf.com/pdf-converter
PDF Forge	http://www.pdfforge.org/pdfcreator
PIX Converter	https://www.coffeecup.com/pixconverter
Publisher to PDF	https://www.publishertopdf.com
RoboBraille	https://www.robobraille.org
XnConvert	https://www.xnview.com/en/xnconvert
Zamzar	https://www.zamzar.com

URL Shorteners and Expanders

Tool	Link
Bit.do	https://bit.do
bitly	https://bitly.com
CheckShortURL	http://checkshorturl.com
GetLinkInfo	http://www.getlinkinfo.com
unFurlr	https://unfurlr.com
Unshorten	https://unshorten.it
Unshorten.link	https://chrome.google.com/webstore/detail/unshortenlink/gbobdaaeaihkghbokihkofcbndhmbdpd?hl=en
urlex	http://urlex.org
Where Does This Link Go?	http://wheredoesthislinkgo.com

Keywords Discovery and Research

Tool	Link
Google Adwords	http://adwords.google.com
Google Keyword Suggest Tool	http://tools.seochat.com/tools/suggest-tool
Google Trends	https://www.google.com/trends
Keyword Discovery	http://www.keyworddiscovery.com
Keyword Spy	http://www.keywordspy.com
KeywordTool	http://keywordtool.io
One Look Reverse Dictionary	http://www.onelook.com/reverse-dictionary.shtml
Word Tracker	https://www.wordtracker.com
Soovle	http://www.soovle.com
Ubersuggest	http://ubersuggest.org

Android Emulators

Tool	Link
Andyroid	https://www.andyroid.net
BlueStacks	https://www.bluestacks.com
GenyMotion	https://www.genymotion.com
Leapdroid	https://leapdroid.en.softonic.com
NoxPlayer	https://www.bignox.com

Virtual Machine

Tool	Link
Buscador Investiagtive Operating System	https://inteltechniques.com/buscador
Linux KVM	https://www.linux-kvm.org/page/Main_Page
Microsoft VMS	https://developer.microsoft.com/en-us/microsoft-edge/tools/vms
Parallels	https://www.parallels.com
QEMU	https://www.qemu.org
Veertu	https://veertu.com
VirtualBox	https://www.virtualbox.org/wiki/Downloads
VMWare	https://www.vmware.com
VMWare ESXi	https://www.vmware.com/products/esxi-and-esx.html
Windows Hyper-V	https://www.microsoft.com/en-us/cloud-platform/server-virtualization
Windows Virtual PC	https://www.microsoft.com/en-us/download/details.aspx?id=3702
Xenserver	https://xenserver.org

Date & Time

Tool	Link
Coder's Tool Box	https://coderstoolbox.net/unixtimestamp
Earth Date to Martian Solar Longtitude	http://www-mars.lmd.jussieu.fr/mars/time/martian_time.html
EpochConverter	https://www.epochconverter.com
Epoch Timestamp Converter	https://www.unixtimestamp.com/index.php
Every Time Zone	http://everytimezone.com
ExcelJet	https://exceljet.net/formula/convert-time-to-time-zone
NASA's HEASARC Tools	https://heasarc.gsfc.nasa.gov/cgi-bin/Tools/xTime/xTime.pl
Online Conversion	http://www.onlineconversion.com/unix_time.htm
Sonnenverlauf	https://www.sonnenverlauf.de
SunCalc	http://suncalc.net
Sun or Moon Rise (US)	http://aa.usno.navy.mil/data/docs/RS_OneYear.php
timeanddate	https://www.timeanddate.de
Timeanddate	https://www.timeanddate.com/worldclock/converter.html
Time Now	http://www.thetimenow.com
TimeStampConvert	http://www.timestampconvert.com
Time Temperature	https://www.timetemperature.com/time-tools-advanced/time-converter-future-date.php
Time Zone Converter	http://www.timezoneconverter.com/cgi-bin/tzc.tzc
Time Zone Converter	http://www.thetimezoneconverter.com
World Time Buddy	https://www.worldtimebuddy.com
World Time Server	https://www.worldtimeserver.com
WolpframAlpha	http://www.wolframalpha.com

Weather

Tool	Link
AccuWeather Global	https://www.accuweather.com/en/world-weather
Aviation Weather Center	https://www.aviationweather.gov
BBC Weather	https://www.bbc.com/weather
Earth	https://earth.nullschool.net
Global Sailing Weather	http://www.globalsailingweather.com
GreatWeather	http://www.greatweather.co.uk
Intellicast	http://www.intellicast.com
MeteoFrance	http://www.meteofrance.com
MetEye	http://www.bom.gov.au/australia/meteye
Mike's Weather Page	http://spaghettimodels.com
NOOA Weather	http://www.noaa.gov/weather
Open Weather Map	https://openweathermap.org
UK Weather Cams	http://www.ukweathercams.co.uk
Ventusky	https://www.ventusky.com
weatherbase	http://www.weatherbase.com
Weather Underground	https://www.wunderground.com
Weather And Climate	https://weather-and-climate.com
Weather.com	https://weather.com
Weather.gov	https://www.weather.gov
weather.org	http://weather.org
Weatherzone.com	http://www.weatherzone.com.au/world
Wetter.com	https://www.wetter.com
Windy.com	https://www.windy.com/?39.538,-76.352,5
wisuki	http://wisuki.com

World Weather	http://worldweather.wmo.int/en/home.html
World Weather and Climate Extremes Archive	https://wmo.asu.edu
World Weather Online	https://www.worldweatheronline.com/lang/en-us
wunderground	https://www.wunderground.com

Barcodes

Tool	Link
Barcode Link	http://www.barcodelink.net
Barcode Reader	https://online-barcode-reader.inliteresearch.com
Barcode Scanner	https://play.google.com/store/apps/details ?id=com.google.zxing.client.android&hl=en_US
CodeReader	https://www.codereadr.com/
IB Scanner	http://www.ibscanner.com/online-barcode-scanner
Online Barcode Reader	https://www.onlinebarcodereader.com
Online Barcode Reader	https://online-barcode-reader.com
QR and Barcode Reader	https://play.google.com/store/apps/details ?id=com.teacapps.barcodescanner&hl=en_US
QR Code Reader and Scanner	https://itunes.apple.com/us/app/ qr-code-reader-and-scanner/id388175979?mt=8
QR Code Scanner	https://webqr.com
Scandit	https://www.scandit.com
ScanMe	https://www.scan.me
Scan – QR Code, Barcode Reaser	https://itunes.apple.com/us/app/ scan-qr-code-barcode-reader/id411206394?mt=8

Analysis

Social Network Analysis

Tool	Link
Gephi	https://gephi.org
Graph Commons	https://graphcommons.com
IBM Analyst Notebook	https://www.ibm.com/us-en/marketplace/analysts-notebook
ORA	http://www.casos.cs.cmu.edu/projects/ora/software.php
Sentinel Visualizer	http://www.fmsasg.com
SocioViz	http://socioviz.net
Visual Investigative Scenarios	https://vis.occrp.org

Geospatial OSINT

Geospatial Research and Mapping Tools

Tool	Link
ACT Map	http://www.actmapi.act.gov.au
AIRBUS WorldDEM	http://www.intelligence-airbusds.com/worlddem-sampledata
ALOS	http://www.eorc.jaxa.jp/ALOS/en/aw3d30
Animaps	http://www.animaps.com
a.placebetween.us	http://a.placebetween.us
aprs	https://aprs.fi
ArcGIS Online	https://www.arcgis.com
Atlasify	http://www.atlasify.com
Baidu Maps	http://map.baidu.com
Batchgeo	http://batchgeo.com
Batch Geocoding	https://www.doogal.co.uk/BatchGeocoding.php
Batch Reverse Geocoding	https://www.doogal.co.uk/BatchReverseGeocoding.php
Bing Maps	http://www.bing.com/maps
Bing Maps Aerial in Google Earth	http://ge-map-overlays.appspot.com/bing-maps/aerial
Bonding Box Drawing Tool	http://automatingosint.com/blog/geographic-bounding-box-drawing-tool
Carto	https://carto.com
Colorbrewer	http://colorbrewer2.org
Convert Latitude/Longitude to Decimal	https://andrew.hedges.name/experiments/convert_lat_long

Coordinate Conversion	http://www.synnatschke.de/geo-tools/coordinate-converter.php
Corona @ CAST	http://corona.cast.uark.edu
CrimeMapping	https://www.crimemapping.com
CrimeReports	https://www.crimereports.com
CrowdMap	https://crowdmap.com
CTLRQ Address Lookup	https://ctrlq.org/maps/address
Custom Satellite View Tools	https://inteltechniques.com/osint/menu.maps.html
Daum Maps	http://map.daum.net
DIgitalGlobe	http://www.digitalglobe.com \|\| https://discover.digitalglobe.com
DigitalGlobe ImageFinder	https://browse.digitalglobe.com/imagefinder
Diva-GIS	http://www.diva-gis.org
Dominoc925	https://dominoc925-pages.appspot.com/mapplets/cs_mgrs.html
doogal	https://www.doogal.co.uk
dronestagram	http://www.dronestagr.am
DualMaps	http://data.mashedworld.com/dualmaps/map.htm
Earth Data	https://search.earthdata.nasa.gov/search
EarthExplorer	https://earthexplorer.usgs.gov
EarthPoint Convert	http://www.earthpoint.us/Convert.aspx
Earth Resources Observation and Science Center - USCG	https://eros.usgs.gov/find-data
Echosec	https://www.echosec.net
EOLI	https://earth.esa.int/web/guest/eoli
esri	http://www.esri.com
Esri Search	https://esri-es.github.io/arcgis-search
Europe Livemap	http://europe.liveuamap.com
Facebook Live Map	https://www.facebook.com/live
Fallingrain	http://www.fallingrain.com/world/index.html
Follow Your World	https://followyourworld.appspot.com
FreeMap Tools	https://www.freemaptools.com/radius-around-point.htm
Geobytes	http://geobytes.com/FreeServices

GeoHack	https://tools.wmflabs.org/geohack/geohack.php
GeoFabrik	http://www.geofabrik.de
GeoGig	http://geogig.org
Geograph	https://www.geograph.org
Geographic Coordinates Converter	http://www.synnatschke.de/geo-tools/coordinate-converter.php
GeoLocate This!	http://geolocatethis.site
GeoNames	http://www.geonames.org
GeoPlaner	http://www.geoplaner.com
GeoSocial Footprint	http://geosocialfootprint.com
GeoVisual Search	https://search.descarteslabs.com
Global Explorer	https://www.globalxplorer.org
Global Gazetteer	http://www.fallingrain.com/world/index.html
Go KML Maps	http://gokml.net/maps#ll=33.467074,-99.528235&z=10&t=h
Google Earth	http://www.google.com/earth
Google Maps	https://www.google.com/maps
Google Maps Downloader	http://www.allmapsoft.com/gmd
Google Maps Streetview Player	http://brianfolts.com/driver
Google My Maps	https://www.google.com/maps/about/mymaps
Gosur Map	http://www.gosur.com/map
GPSVisualizer	http://www.gpsvisualizer.com
GrassGIS	http://grass.osgeo.org
Here	http://here.com
HibeBikeMap	http://hikebikemap.org
Historic Aerials	https://www.historicaerials.com
Hivemapper	https://hivemapper.com
Hyperlapse	https://github.com/TeehanLax/Hyperlapse.js
Imergis	http://www.imergis.nl
Indian Geo-Platform of ISRO	http://bhuvan.nrsc.gov.in/data/download/index.php
INPE Image Catalog	http://www.dgi.inpe.br/CDSR
Inspire Geoportal	http://inspire-geoportal.ec.europa.eu
InstantAtlas	http://www.instantatlas.com

Instant Google Street View	http://www.instantstreetview.com
Inteltechniques Custom Mapping Tools	https://inteltechniques.com/osint/maps.html
Kartograph	http://kartograph.org
Land Cover	http://landcover.org
Land Information New Zealand	https://data.linz.govt.nz
Landsat Look	https://landsatlook.usgs.gov/viewer.html
Land Viewer	https://eos.com/landviewer
Latlong	https://www.latlong.net
Leaflet	http://leafletjs.com
Libra	https://libra.developmentseed.org
Liveuamap	http://liveuamap.com
MapAList	http://mapalist.com
MapBox	https://www.mapbox.com
Mapchart.net	https://mapchart.net
Map Checking	https://www.mapchecking.com
Map Developers	https://www.mapdevelopers.com
Maperitive	http://maperitive.net
MapHub	https://maphub.net
Mapillary	https://www.mapillary.com
mapkit	https://mapkit.io
Mapline	https://mapline.com
Map Puzzle	http://www.mappuzzle.se
Map Overlays for Google Earth	http://www.mgmaps.com/kml/#view
Mapquest	https://www.mapquest.com
meetways	https://www.meetways.com
MgMaps	http://mgmaps.com/kml/#view
Military Grid Reference System Coordinates	https://dominoc925-pages.appspot.com/mapplets/cs_mgrs.html
Modest Maps	http://modestmaps.com
Movable Type Scripts	http://www.movable-type.co.uk/scripts/latlong-os-gridref.html
MyGeoPosition	http://mygeoposition.com

NASA Earth Observatory	https://earthobservatory.nasa.gov
Naver Maps	https://map.naver.com
NEXRAD Data Archive, Inventory, and Access	https://www.ncdc.noaa.gov/nexradinv
NGA GEOINT	https://github.com/ngageoint
NOAA CLASS	https://www.bou.class.noaa.gov/saa/products/catSearch
NOAA DataViewer	https://coast.noaa.gov/dataviewer
NOAA Digital Coast	https://coast.noaa.gov/digitalcoast
OpenLayers	http://openlayers.org
OpenStreetCam	https://www.openstreetcam.org/map/
OpenStreetMap	http://www.openstreetmap.org
Overpass Turbo	https://overpass-turbo.eu
pattrn	http://pattrn.co
Photo Maps	http://photo-map.ru
Planet Explorer	https://www.planet.com/explorer
Polymaps	http://polymaps.org
Perry Castaneda Library	https://www.lib.utexas.edu/maps
Old Maps Online	http://www.oldmapsonline.org
Open Railway Map	https://www.openrailwaymap.org
Open Street Cam	http://openstreetcam.org
Open Street Map	http://www.openstreetmap.org
QGIS	http://qgis.org
QuickMaps	https://chrome.google.com/webstore/detail/quick-maps/bgbojmobaekecckmomemopckmeipecij
Radiant Earth	https://radiant.earth
Research UN Maps	http://research.un.org/en/maps
SASGIS	http://www.sasgis.org
Scribble Maps	http://scribblemaps.com
Sentinel2Look Viewer	https://landsatlook.usgs.gov/sentinel2
Sentinel Hub Playground	http://apps.sentinel-hub.com/sentinel-playground
StoryMap	https://storymap.knightlab.com
StoryMaps	http://storymaps.arcgis.com/en

Tableau	http://www.tableausoftware.com
TerraPattern	http://www.terrapattern.com
TerraServer	https://www.terraserver.com
Travel by Drone	http://travelbydrone.com
US Naviguide	http://www.usnaviguide.com
ViaMichelin	http://www.viamichelin.com
View in Google Earth	http://www.mgmaps.com/kml/#view
VITO Free Satellite Imagery	http://www.vito-eodata.be/PDF/portal/Application.html
Walking Directions	https://www.foxtons.co.uk/tools/walking_directions.html
WarWire	https://www.warwire.net
Wego.here	https://wego.here.com
Wikimapia	http://wikimapia.org
World Aeronautical Database	http://worldaerodata.com
World Map Creator	http://worldmapcreator.com
WorldMap Harvard	http://worldmap.harvard.edu
Yahoo Maps	https://maps.yahoo.com
Yandex Maps	https://yandex.ru/maps
YourNavigation	http://yournavigation.org
Zeemaps	https://www.zeemaps.com
Zoom Earth	https://zoom.earth

Interesting Maps

Tool	Link
ACLED Dashboard	https://www.acleddata.com/dashboard
ACT Government Incidents Map	http://esa.act.gov.au/community-information/incidents-map
A World of Disputed Territories	http://metrocosm.com/disputed-territories-map.html
Crime Mapping (Police.uk)	https://www.police.uk
Disputed Territories	http://metrocosm.com/disputed-territories-map.html
Global Fishing Watch	http://globalfishingwatch.org/map
Global Incident Map	http://www.globalincidentmap.com
IMB Piracy & Armed Robbery Map	https://www.icc-ccs.org/piracy-reporting-centre/live-piracy-map
Live Piracy Map	http://www.icc-ccs.org/piracy-reporting-centre/live-piracy-map
Live Earthquakes Map	http://quakes.globalincidentmap.com
Mapping the Flow of International Trade	http://www.visualcapitalist.com/interactive-mapping-flow-international-trade
MissileMap	http://nuclearsecrecy.com/missilemap
N2YO.com	http://www.n2yo.com
National Geographic Map Stories	https://www.nationalgeographic.com/maps
Newspaper Map	https://newspapermap.com
Nukemap	http://nuclearsecrecy.com/nukemap
Relief Web Maps	https://reliefweb.int/countries
Risk Map	https://www.riskmap.com
Roadworks	https://roadworks.org
Roman Heritage	http://sites.romaheritage.co.uk

RSOE EDIS Alert Map	http://hisz.rsoe.hu/alertmap/index2.php
Secret Bases	https://www.secret-bases.co.uk/google-earth.htm
Snapchat Map	https://map.snapchat.com
Space Near Us	http://spacenear.us
Strava Global Heatmap	https://www.strava.com/heatmap#7.00/-120.90000/38.36000/hot/all
Tracker.habhub	https://tracker.habhub.org
The True Size Of	https://thetruesize.com
Wifi SPC	https://wifispc.com
World Aero Data	http://worldaerodata.com

Privacy and Security

General Privacy Tools and Resources

Tool	Link
Abine	https://www.abine.com
AccountKiller	https://www.accountkiller.com
Background Checks	http://backgroundchecks.org
BleachBit	https://www.bleachbit.org
CCleaner	https://www.piriform.com/ccleaner
Centralised Place for Privacy Resources	https://themanyhats.club/centralised-place-for-privacy-resources
CleanMyMac	https://macpaw.com/cleanmymac
ClearConsole	https://addons.mozilla.org/en-US/firefox/addon/clear-console
Click&Clean	https://addons.mozilla.org/en-US/firefox/addon/clickclean
deseat	https://www.deseat.me
Dock	https://dock.io
Epic.org Privacy Tools	https://epic.org/privacy/tools.html
Eraser	http://eraser.heidi.ie
GNU PG	https://www.gnupg.org/download/index.html
Guardian Project	https://guardianproject.info
HotCleaner	https://www.hotcleaner.com
justdeleteme	http://justdelete.me
Me and My Shadow	https://myshadow.org
My Data Request	https://mydatarequest.com
MyPermissions	https://mypermissions.com
OptOutPrescreen	https://www.optoutprescreen.com

Peerblock	http://forums.peerblock.com
PixelPrivacy	https://pixelprivacy.com
Pribot	https://pribot.org
Prism Break	https://prism-break.org
Privacy Checker	http://www.privacychecker.nl/en
Privacy Pal	http://www.privacypal.co
Privacy Rights Clearinghouse	https://www.privacyrights.org
Privacy Tools	https://www.privacytools.io
Privazer	http://privazer.com
Opt-Out Doc	https://docs.google.com/spreadsheets/d/1UY9U2CJ8Rnz0CBrNu2iGV3yoG0nLR8mLINcnz44XESI/edit#gid=1864750866
Social Media Leak	https://robinlinus.github.io/socialmedia-leak
TOSBack	https://tosback.org
ToSDR	https://tosdr.org
Verexif	http://www.verexif.com
What Facebook Thinks You Like	https://chrome.google.com/webstore/detail/what-facebook-thinks-you/eoknmaajkanapojcdeccofmeimpddoim?hl=en

Secure Browsing

Tool	Link
Adblock Plus	https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/?src=search
Am I Unique?	https://amiunique.org
anonymoX	https://www.anonymox.net
Avast	https://www.avast.com/en-us/secure-browser
Bitdefender Traffic Light	https://www.bitdefender.co.uk/solutions/trafficlight.html
Blender	https://addons.mozilla.org/en-US/firefox/addon/blender-1
Blur	https://addons.mozilla.org/en-US/firefox/addon/donottrackplus/?src=search
Brave	https://brave.com
Browserleaks	https://browserleaks.com
Browserscope	http://www.browserscope.org
BrowserSpy	http://browserspy.dk
Citrix	https://www.citrix.com/virtualization/secure-browser.html
Click & Clean	https://chrome.google.com/webstore/detail/clickclean/ghgabhipcejejjmhhchfonmamedcbeod?hl=en
Cliqz	https://cliqz.com
Cocoon	https://getcocoon.com
Comodo's Dragon	https://www.comodo.com/home/browsers-toolbars/browser.php
Cookie AutoDelete	https://addons.mozilla.org/en-US/firefox/addon/cookie-autodelete/?src=search
Country Flags & IP Whois	https://addons.mozilla.org/en-US/firefox/addon/country-flags-ip-whois/?src=search
Credit Card Nanny	https://chrome.google.com/webstore/detail/credit-card-nanny/lfmmjpapolbaaddobpnlcjkgchmhhoog

Decentraleyes	https://addons.mozilla.org/en-US/firefox/addon/decentraleyes/?src=rating
Disconnect	https://addons.mozilla.org/en-US/firefox/addon/disconnect/?src=featured \|\| https://disconnect.me/disconnect
Doileak	https://www.doileak.com
Epic Privacy Browser	https://www.epicbrowser.com
Ericom	https://www.ericom.com/solutions/browser-isolation
Extension Source Viewer	https://addons.mozilla.org/en-US/firefox/addon/crxviewer/?src=rating
Firefox Lightbeam	https://addons.mozilla.org/en-GB/firefox/addon/lightbeam
Forget Me Not	https://addons.mozilla.org/en-US/firefox/addon/forget_me_not/?src=featured
Freenet	https://freenetproject.org/index.html
Globus	https://globus-vpn-browser.en.softonic.com
Ghostery	https://addons.mozilla.org/en-US/firefox/addon/ghostery/?src=featured
HTTPs Everywhere	https://www.eff.org/https-everywhere
I2P	https://geti2p.net/en
IPLeak	https://www.ipleak.net
Iridium	https://iridiumbrowser.de
KeeFox	https://addons.mozilla.org/en-US/firefox/addon/keefox
Kimetrak	https://addons.mozilla.org/en-US/firefox/addon/kimetrak/?src=search
Link Cleaner	https://addons.mozilla.org/en-US/firefox/addon/link-cleaner
Netcraft Anti-Phishing Extension	https://addons.mozilla.org/en-US/firefox/addon/netcraft-toolbar
NoScript	https://noscript.net
No-Script Suite Lite	https://chrome.google.com/webstore/detail/no-script-suite-lite/ahnanjpbkghcdgmlchbcfoiefnifjeni?hl=en
Panopticlick	https://panopticlick.eff.org
Passport	https://addons.mozilla.org/en-US/firefox/addon/passbolt/?src=featured
Policeman	https://addons.mozilla.org/en-US/firefox/addon/policeman
Privacy Badger	https://addons.mozilla.org/en-US/firefox/addon/privacy-badger17/?src=search

Privacy & Security Add-ons	https://addons.mozilla.org/en-US/firefox/extensions/privacy-security
Privacy Tab	https://addons.mozilla.org/en-US/firefox/addon/private-tab/?src=rating
Private Bookmarks	https://addons.mozilla.org/en-US/firefox/addon/webext-private-bookmarks/?src=search
Safe Browser	https://chrome.google.com/webstore/detail/safe-browser/lapbdblogmakkmcnkacalmpoljnofnnj?hl=en
Safe Browsing	https://chrome.google.com/webstore/detail/safe-browsing/ecpnacfdmkfdabpdpbnnacjfdfcldklf?hl=en
Safe Web	https://safeweb.norton.com
Script Safe	https://chrome.google.com/webstore/detail/scriptsafe/oiigbmnaadbkfbmpbfijlflahbdbdgdf?hl=en
Self-Destructing Cookies	https://addons.mozilla.org/en-US/firefox/addon/self-destructing-cookies
Simple Blocker	https://chrome.google.com/webstore/detail/simple-blocker/akfbkbiialncppkngofjpglbbobjoeoe
SRWare Iron	http://www.srware.net/en/software_srware_iron.php
SSleuth	https://addons.mozilla.org/en-US/firefox/addon/ssleuth/?src=rating
Sucuri Free Website Malware and Security Scanner	https://sitecheck.sucuri.net
Tor Project	https://www.torproject.org
Trust Wave	https://www.trustwave.com/Products/SecureBrowsing
UBlock Origin	https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/?src=search
UMatrix	https://addons.mozilla.org/en-US/firefox/addon/umatrix
US-CERT	https://www.us-cert.gov/publications/securing-your-web-browser
User-Agent Switcher	https://addons.mozilla.org/en-US/firefox/addon/user-agent-switcher-revived/?src=search
Vanilla Cookie Manager	https://chrome.google.com/webstore/detail/vanilla-cookie-manager/gieohaicffldbmiilohhggbidhephnjj?hl=en
Webutation	http://www.webutation.net
What browser am I using?	http://www.whatbrowseramiusing.co
WhatIsMyBrowser	https://www.whatismybrowser.com

WOT	https://www.mywot.com

Ads and Tracking Blockers

Tool	Link
AdblockPlus	https://adblockplus.org
AskBlocker	https://adamlynch.com/askblocker
Blokada	http://blokada.org
Disconnect	https://disconnect.me
Do Not Track	http://donottrack.us
Do Not Track Me Google	https://chrome.google.com/webstore/detail/dont-track-me-google/gdbofhhdmcladcmmfjolgndfkpobecpg?hl=en
Ghostery	https://www.ghostery.com
Nixory	http://nixory.sourceforge.net
No Script	https://noscript.net
Panopticlick	https://panopticlick.eff.org
PixelBlock	https://chrome.google.com/webstore/detail/pixelblock/jmpmfcjnflbcoidlgapblgpgbilinlem?hl=en
Privacy Badger	https://www.eff.org/privacybadger
Trackography	https://trackography.org
uBlock	https://www.ublock.org

Blocking of Currency Miners

Tool	Link
CryptoPrevent Malware Prevention	https://www.foolishit.com/cryptoprevent-malware-prevention/#gsc.tab=0
How-to Geek	https://www.howtogeek.com/334018/how-to-block-cryptocurrency-miners-in-your-web-browser
Malware Bytes	https://www.malwarebytes.com/lp/sem/en/?c=cj&s=2786910&aid=11971602&k=11971602&utm_source=cj&utm_medium=aff&utm_content=11971602&utm_campaign=AFF-CJ_2786910&tracking=cj&x-wts=cj&x-affid=2786910&ADDITIONAL_AFFID=cj-2786910
minerBlock	https://chrome.google.com/webstore/detail/minerblock/emikbbbebcdfohonlaifafnoanocnebl
No Coin	https://chrome.google.com/webstore/detail/no-coin-block-miners-on-t/gojamcfopckidlocpkbelmpjcgmbgjcl
NoScript	https://addons.mozilla.org/en-US/firefox/addon/noscript
Opera	https://www.opera.com

Private Search Engines and Private Searching

Tool	Link
Disconnect Search	https://disconnect.me/search
Discrete search	https://www.discretesearch.com
Duck Duck Go	https://duckduckgo.com
Gibiru	http://www.gibiru.com
Lukol	https://www.lukol.com
MetaGer	https://metager.de
Oscobo	https://oscobo.co.uk
peekier	https://peekier.com
Search encrypt	https://www.searchencrypt.com
Searx.me	https://searx.me
Startpage by ixquick	https://www.ixquick.com
Swisscows	https://swisscows.com
Qwant	https://www.qwant.com

Secure OS

Tool	Link
Qubes	https://www.qubes-os.org
Tails	https://tails.boum.org
whonix	https://www.whonix.org

Backup Tools

Tool	Link
Acronis	https://www.acronis.com
BackBlaze	https://www.backblaze.com
Carbonite	https://www.carbonite.com
Crashplan	https://www.crashplan.com
Dropbox	https://www.dropbox.com/?landing=dbv2
Handy Backup	https://www.handybackup.net/backup-website.shtml
IBackup	https://www.ibackup.com
IDrive	https://www.idrive.com
Jungle Disk	https://www.jungledisk.com
Mozy	https://mozy.com/#slide-11
Norton Online backup	https://nobu.backup.com/session/new
OpenDrive	https://www.opendrive.com
SiteGround	https://www.siteground.com/tutorials/getting-started/backup-and-restore-tool
Site Vault	http://www.site-vault.com
Spideroak: One	https://spideroak.com/one
SOS Online Backup	https://www.sosonlinebackup.com

Secure Communication Tools

Tool	Link
Adium	https://adium.im
Chanty	https://www.chanty.com
Chatsecure	https://chatsecure.org
Crypto.cat	https://crypto.cat
Fleep	https://fleep.io
Google Hangouts	https://hangouts.google.com
Go To Meeting	https://www.gotomeeting.com
Hipchat	https://www.stride.com
Join.me	https://www.join.me
Mailbird	https://www.getmailbird.com
Pidgin	https://www.pidgin.im
Realtime Board	https://realtimeboard.com
Signal	https://signal.org
Silent circle	https://www.silentcircle.com
Skype for Business	https://www.skype.com/en/business
Slack	https://slack.com/r/02tltzm1-02tpl6m9
Spideroak: Semaphor	https://spideroak.com/semaphor
Surveilliance Self Defense	https://ssd.eff.org
Syndie	http://syndie.i2p2.de
Telegram	https://telegram.org
Tibbr	http://www.tibbr.com
Unseen.is	https://unseen.is
Workfront	https://www.workfront.com
Yammer	https://www.yammer.com

E-mail Security

Tool	Link
10minutemail	https://10minutemail.com
20minutemail	http://www.20minutemail.com
Anonymouse	http://anonymouse.org
Ashley Madison Hack	https://ashley.cynic.al
BreachAlarm	https://breachalarm.com
Disposable-email-domains	https://github.com/martenson/disposable-email-domains/blob/master/disposable_email_blacklist.conf
Disposable-email-provider-domains	https://gist.github.com/michenriksen/8710649
E4ward	http://e4ward.com
EmailOnDeck	https://www.emailondeck.com
Enigmail	https://www.enigmail.net
Gawker Hack Email Check	https://labs.duo.com/gawker
Gmelius for Inbox by Gmail	https://chrome.google.com/webstore/detail/gmelius-for-inbox-by-gmai/dlbjhjnahgmigifoggidegpakbcjomgg
Googligan Checker	https://gooligan.checkpoint.com
Gotcha	https://gotcha.pw
GPG Tools	https://gpgtools.org
Guerrilla Mail	https://www.guerrillamail.com
Hacked Emails	https://hacked-emails.com
Have I Been Pwned	https://haveibeenpwned.com
Have I Been Sold	https://haveibeensold.app

HPI Identity Leak Checker	https://sec.hpi.uni-potsdam.de/ilc/search;jsessionid=A94B3A03C67B00F3B0FADB4A8C08E6FA
InboxBear	https://inboxbear.com
Leaked Source	https://leakedsource.ru
Lockbin	https://lockbin.com
Mailbox	https://mailbox.org
Mailinator	http://www.mailinator.com
Mailvelope	https://www.mailvelope.com
MyTrashMail	http://mytrashmail.com
Open PGP	https://www.enigmail.net/index.php/en
Pixel Block	https://chrome.google.com/webstore/detail/pixelblock/jmpmfcjnflbcoidlgapblgpgbilinlem
ProtonMail	https://protonmail.com
Psbdmp.ws	https://psbdmp.ws//
Scamdex	http://www.scamdex.com
Sneakemail	https://sneakemail.com
Snusbase	https://snusbase.com
Streak SecureGmail	https://www.streak.com/securegmail
Sudo App	https://sudoapp.com
Tempr.email	https://tempr.email
Thunderbird	https://www.mozilla.org/en-US/thunderbird
TrashMail	https://trashmail.com
Unseen.is	https://unseen.is
Vigilante	https://www.vigilante.pw
ZMail	http://zmail.sourceforge.net

Phone Security

Tool	Link
Hushed	https://hushed.com
Leaked Source	https://leakedsource.ru
Receive SMS	https://receive-sms.com
Receive SMS Online	http://receive-sms-online.com
Receive SMS Online	https://www.receivesmsonline.net
SMS Sellaite	http://sms.sellaite.com
Snusbase	https://snusbase.com
Sudo App	https://sudoapp.com
Vigilante	https://www.vigilante.pw

Password Management and Secure Login

Tool	Link
1Password	https://1password.com
Dashlane	https://www.dashlane.com
KeePass Password Safe	http://keepass.info
Last Pass	https://lastpass.com
Master Password	http://masterpasswordapp.com
Password Alert	https://chrome.google.com/webstore/detail/password-alert/noondiphcddnnabmjcihcjfbhfklnnep
Have I Been Pwned	https://haveibeenpwned.com/Passwords
Spideroak: Encrypt	https://spideroak.com/encryptr
Two Factor Auth	https://twofactorauth.org
Unseen.is	https://unseen.is
What Facebook Thinks You Like	https://chrome.google.com/webstore/detail/what-facebook-thinks-you/eoknmaajkanapojcdeccofmeimpddoim?hl=en
WOT	https://www.mywot.com
ZMail	http://zmail.sourceforge.net

Encryption Tools

Tool	Link
AES Crypt	https://www.aescrypt.com
Axcrypt	https://www.axcrypt.net
BitLocker	https://www.microsoft.com/en-in/download/details.aspx?id=7806
boxcryptor	https://www.boxcryptor.com
CertainSafe	https://certainsafe.com/digital-safety-deposit-box
Challenger	https://encryption-software.de/challenger/en/index.html
Cryptainer LE	https://www.cypherix.com/cryptainerle
CryptoExpert	https://www.cryptoexpert.com
CryptoForge	http://www.cryptoforge.com
Dekart	https://www.dekart.com/free_download
DiskCryptor	https://diskcryptor.net/wiki/Downloads
Encrypted Cloud	https://www.encryptedcloud.com
FileVault	https://support.apple.com/en-us/HT204837
Folder Lock	http://www.newsoftwares.net/folderlock
Intercrypto	https://www.intercrypto.com
Rohos	https://www.rohos.com
Secure IT	https://www.cypherix.com/secureit2000
SecurStick	http://www.withopf.com/tools/securstick
Steganos	https://www.steganos.com/de/steganos-safe-19
Streak SecureGmail	https://www.streak.com/securegmail
Symantec Drive Encryption	https://www.symantec.com/smb
Veracrypt	https://www.veracrypt.fr/en/Home.html

7-Zip	https://www.7-zip.org/download.html

Secure File Sharing

Tool	Link
Box	https://www.box.com
DropBox	https://www.dropbox.com/?landing=dbv2
Drop Send	https://www.dropsend.com
Egnyte	https://www.egnyte.com
Google Drive	https://www.google.com/drive
HighTail	https://www.hightail.com
Just Cloud	http://www.justcloud.com
OneHub	https://www.onehub.com
OpenDrive	https://www.opendrive.com
Securesha	https://securesha.re
Send This File	https://www.sendthisfile.com
Share File	https://www.sharefile.com
Smart Room	https://smartroom.com
Sugar Sync	https://www2.sugarsync.com
4Shared	https://www.4shared.com

VPN Services

Tool	Link
Box PN	https://boxpn.com
CryptoStorm	https://cryptostorm.is/#section5
CyberGhost	https://www.cyberghostvpn.com
ExpressVPN	https://www.expressvpn.com
HideMyAss	https://www.hidemyass.com
Hoxx	https://hoxx.com
Hotspot Shield	https://www.hotspotshield.com
IPVanish	https://www.ipvanish.com
Mullvad	https://mullvad.net
NordVPN	https://nordvpn.com
Overplay	https://www.overplay.net/en/products/vpn
Personal VPN	https://www.personalvpn.com
Pure VPN	https://www.purevpn.com
TorGuard	https://torguard.net
TunnelBear	https://www.tunnelbear.com
Private Internet Access	https://www.privateinternetaccess.com
Speedify	http://speedify.com/desktop-vpn
Strong VPN	https://strongvpn.com/plans.htm
UnoTelly	https://www2.unotelly.com
Viking VPN	https://vikingvpn.com
VPN Unlimited	https://www.vpnunlimitedapp.com
Vypr VPN	https://www.goldenfrog.online/vyprvpn
Windscribe	https://windscribe.com

ZenMate	https://zenmate.com
ZenVPN	https://zenvpn.net/en

VPN Texting

Tool	Link
Check IP	https://www.perfect-privacy.com/check-ip
DNS Leak	https://www.dnsleaktest.com
DNS Leak Test	http://dnsleak.com
Email Leak Test	http://emailipleak.com
IPCheck	http://ip-check.info
IPLeak	https://ipleak.net
IPv6 Leak Test	http://ipv6leak.com

Proxy Tools

Tool	Link
4everproxy	http://www.4everproxy.com
anype	http://www.anype.com
FilterBypass	https://www.filterbypass.me
Hide.me	https://hide.me/en/proxy
HideMyAss Proxy	https://www.hidemyass.com/proxy
Premium Proxy	https://premproxy.com
Proxy4Free	http://www.proxy4free.com
ProxySite	https://www.proxysite.com
Public Proxy Servers	http://www.publicproxyservers.com

Antivirus Software

Tool	Link
Avast Pro Antivirus	https://www.avast.com/en-us/pro-antivirus
AVG Internet Security Unlimited	https://support.avg.com/support_Protection?l=en
BitDefender Antivirus Plus	https://www.bitdefender.com/media/html/2018/cl50off-opt/?pid=50off&cid=aff\|c\|ir
BullGuard	https://www.bullguard.com/products/bullguard-antivirus.aspx
ESET Internet Security	https://www.eset.com/us/newyear/?ref=AFC-CJ&attr=7603059&pub=12800315&shop=521pxCDDNg
ESET NOD32 Antivirus	https://www.eset.com/us/home/antivirus
F-Secure Anti-Virus	https://www.f-secure.com/en_US/web/home_us/anti-virus
McAfee Antivirus Plus	https://www.mcafee.com/consumer/en-us/promos/sem/l1144/0s/01/01/a/01_sl125.html
McAfee Total Protection	https://www.mcafee.com/consumer/en-us/store/m0/catalog/mtp_521/mcafee-total-protection.html
Norton Antivirus Basic	https://us.norton.com/norton-antivirus
Norton Security Deluxe	https://us.norton.com/norton-security-antivirus
Sohos Home Premium	https://home.sophos.com
Trend Micro Antivirus + Security	https://www.trendmicro.com/en_us/forHome/products/antivirus-plus.html
Webroot SecureAnywhere Antivirus	https://www.webroot.com/us/en/home/products/av

Other Security Tools

Tool	Link
Angry IP Scanner	http://angryip.org
Cymon	https://cymon.io
Defacer	https://defacer.id
ID Ransomware	https://id-ransomware.malwarehunterteam.com
InSpectre	https://www.grc.com/inspectre.htm
jotti	https://virusscan.jotti.org
Malwarebytes Anti-Rootkit Beta	https://www.malwarebytes.com/antirootkit
NoMoreRansom	https://www.nomoreransom.org
Open DNS	https://www.opendns.com/home-internet-security
OSSEC	https://ossec.github.io
Pulsedive	https://pulsedive.com
Security-in-a-box	https://securityinabox.org
Snort	https://www.snort.org
Tech Solidarity	https://techsolidarity.org
ThreatCrowd	https://threatcrowd.org
Threatglass	http://www.threatglass.com
urlquery	https://urlquery.net
Virus Total	https://www.virustotal.com
W3bin	https://w3bin.com
Zone-h	http://www.zone-h.org

Copyright and Takedowns

Tool	Link
Copyscape	https://www.copyscape.com/compare.php
Copyright.gov	https://www.copyright.gov
Copyright Information	http://www.copyrightinformation.org/the-copyright-alert-system
Copywrited.com	https://www.copyrighted.com
DMCA	https://www.dmca.com/Takedowns.aspx
DMCA Pro	http://dmca.pro
Google Webmasters	https://www.google.com/webmasters/#?modal_active=none
Hack Hunter	https://www.hack-hunt.com
Link Killer (Fresh Killer)	http://killer.freshface.cz
Lumen Database	https://lumendatabase.org
Whois Ad-ons	https://addons.mozilla.org/en-US/firefox/search/?q=whois&appver=&platform=
MyVows	https://myows.com
NPPA	https://nppa.org/page/5617
Patent Trademark Laws	http://www.patent-trademark-law.com/copyrights/plagiarism-take-down-stolen-content/cease-desist-dmca-takedown
Plague Hunter	https://www.plaghunter.com
XDMCA Takedown Tool	http://xdmca.com

Researching Leaks

Tool	Link
BalkanLeaks	https://balkanleaks.eu
Cryptome	https://cryptome.org
DataBreaches	https://www.databreaches.net
FindMySnap	http://findmysnap.com
GLOBALLEAKS	https://www.globaleaks.org
OCCRP Data	https://data.occrp.org
Offshore Leaks	https://offshoreleaks.icij.org
Public Library of US Diplomacy	https://search.wikileaks.org/plusd
WELEAKINFO	https://weleakinfo.com
Wikileaks	https://wikileaks.org
Wikileaks Advanced Search	https://search.wikileaks.org/advanced
WikiSpooks	https://wikispooks.com

Research and Recon Tools

Research and Data Recon Tools

Tool	Link
AutOISNT	https://github.com/bharshbarger/AutOSINT
Belati	https://github.com/aancw/Belati
Buscador	https://inteltechniques.com/buscador
dataspoit	https://github.com/DataSploit/dataspoit
FAW Project	https://it.fawproject.com
Inquisitor	https://github.com/penafieljlm/inquisitor
Int-Rec-Pack	https://github.com/NullArray/IntRec-Pack
Intrigue	http://intrigue.io
Maltego	https://www.paterva.com/web7
OSINT Browser	http://osirtbrowser.com
osintstalker	https://github.com/milo2012/osintstalker
OSINT-SPY	https://github.com/SharadKumar97/OSINT-SPY
OSINT Toolkit	https://osinttoolkit.github.io
osrframework	https://github.com/i3visio/osrframework
Paliscope	https://www.paliscope.com
Recon-ng	https://bitbucket.org/LaNMaSteR53/recon-ng
Scumblr	https://github.com/Netflix/Scumblr
Social Recon	https://www.kitploit.com/2018/01/social-recon-investigate-online.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+PentestTools+%28PenTest+Tools%29
Spiderfoot	http://www.spiderfoot.net
theharvester	https://github.com/laramies/theHarvester

XRay	https://n0where.net/network-osint-gathering-tool-xray

OSINT Tools Lists

OSINT Tools Lists

Tool	Link
101+ OSINT Resources for Investigators (i-sight)	https://i-sight.com/resources/101-osint-resources-for-investigators
Aware Online Academy OSINT Links	https://aware-online.com/academy/osint-links
Awesome OSINT	https://github.com/jivoi/awesome-osint
Awesome_osint	https://github.com/Ph055a/awesome_osint
Bellingcat OSINT Links	https://docs.google.com/document/d/1BfLPJpRtyq4RFtHJoNpvWQjmGnyVkfE2HYoICKOGguA/edit
Bruno Mortier Sources	https://start.me/p/3g0aKK/sources
Bruno Mortier Sources CNTY	https://start.me/p/W2kwBd/sources-cnty
CiberPatrulla	https://ciberpatrulla.com/links
DFIR Training Tool Directory	https://www.dfir.training/index.php/tools/advanced-search
Digital intelligence Research Tools	https://atlas.mindmup.com/digintel/digital_intelligence_training/index.html
Emmanuelle Welch Dating apps and sites for investigators	https://start.me/p/VRxaj5/dating-apps-and-sites-for-investigators
HR Sourcing Toolbox	https://hrsourcingtoolbox.wixsite.com/main
Julia Bayer Verification Toolset	https://start.me/p/ZGAzN7/verification-toolset
inteltechniques Internet Search Links	https://inteltechniques.com/menu.links.html
MidaSearch OSINT Websites	https://midasearch.org/osint-websites
Netbootcamp OSINT Tools	https://netbootcamp.org/osinttools

Onstrat OSINT Starting Points	http://www.onstrat.com/osint/#startingpoints
OSINT Browser Plugins	https://github.com/IVMachiavelli/OSINT-Browser-Plugins
OSINT Framework	http://osintframework.com
OSINT Link	http://osint.link
OSINT Post	https://osintpost.com
OSINT Team Links	https://github.com/IVMachiavelli/OSINT_Team_Links
RBA Business Information Resources	http://www.rba.co.uk/sources
Research Clinic	http://www.researchclinic.net
Reuser OSINT Discovery Toolkit	http://rr.reuser.biz
Startme Open Source Investigative Tools by Malachy Browne	https://start.me/p/gyvaAJ/open-source-investigative-tools
Startme OSINT Technisette	https://start.me/p/m6XQ08/osint \|\| https://start.me/p/nRQNRb/addons
Sprp77 Awesome OSINT	https://drive.google.com/drive/folders/0BwyWDQ59jRVGMFp3UnBfeUEzanM
Toddington Resources	https://www.toddington.com/resources
Tomoko Discovery Tools List	https://tomokodiscovery.com/free-tools-osint-socmint-dark-web-darknet-tor-bitcoin
ToolsInsight	http://www.toolsinsight.com
Uk-osint	http://www.uk-osint.net/addons.html



Contact

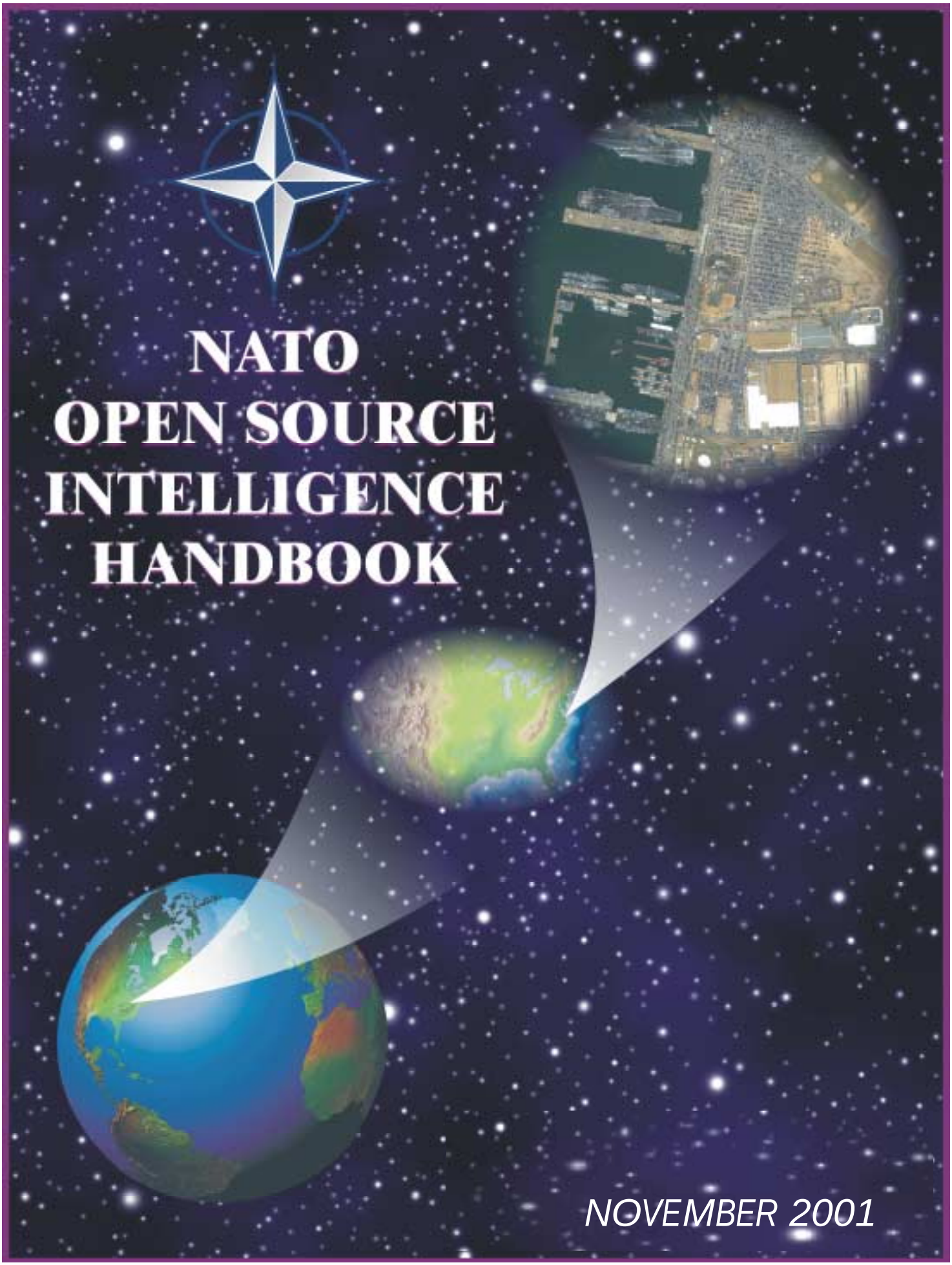
Chris Pallaris

Director

i-intelligence

+41 (0) 43 243 3849 | info@i-intelligence.eu

www.i-intelligence.eu | @i_intelligence


NATO
OPEN SOURCE
INTELLIGENCE
HANDBOOK
NOVEMBER 2001

This Page Is Intentionally Left Blank

PREFACE



This publication provides preliminary joint and coalition training information on the subject of Open Source Intelligence (OSINT). It discusses the fundamentals of OSINT support to both the all-source intelligence process, and to the unclassified intelligence requirements of operators, logisticians, and civilian organizations participating in joint and coalition operations. The focus is on relevant information that can be obtained legally and ethically from the public and private sector, and that is not classified in its origin or processing. The information may become classified in relation to the commander's intent or its association with classified information when it is rightly blended into all-source intelligence reports.

This publication has been prepared under my direction as the Supreme Allied Commander, Atlantic, in collaboration with staff from the Supreme Allied Commander, Europe (SACEUR). This publication has benefited greatly from the continued collaboration between my staff and the staff of Open Source Solutions Inc. With the publication of this document and its companions, the *Intelligence Exploitation of the Internet* and the *NATO OSINT Reader*, commanders and their staffs will have basic guidance for the development of OSINT.

The increasingly robust array of open sources available to all staffs enable commanders at all levels to attempt to satisfy their information requirements themselves rather than immediately directing Requests for Information (RFIs) elsewhere. This manual outlines a systematic approach to OSINT exploitation.

This information is relevant to all NATO commands, task forces, member nations, civil-military committees and working groups, and such other organizations that may be planning or engaged in combined joint operations.

W. F. KERNAN
General, U.S. Army

This Page Is Intentionally Left Blank

Table of Contents

EXECUTIVE SUMMARY **V**
CHAPTER I **1**
OPEN SOURCE INTELLIGENCE AND JOINT OR COALITION OPERATION **1**
Introduction 1
Definitions 2
21st Century Information Operations 3

CHAPTER II **5**
PRIVATE SECTOR INFORMATION OFFERINGS **5**
SECTION A. SOURCES **5**
Traditional Media Sources 5
Commercial Online Premium Sources 6
Other Forms of Commercial Online Information 8
Grey Literature 8
Overt Human Experts and Observer 9
Commercial Imagery 9
Defining Source Access Requirements (Dangers of Pay-per-View) 11
SECTION B. SOFTWARE **12**
Software Hierarchy 12
SECTION C. SERVICES **13**
Collection Services 13
Processing Services 13
Analysis & Production Services 13
Services Examples 14

CHAPTER III **15**
THE OPEN SOURCE INTELLIGENCE CYCLE **15**
SECTION A. OSINT PLANNING AND DIRECTION **15**
Overview 15
Organizations and Responsibilities 15
Requirements Definition 16
Evaluation and Feedback 17
SECTION B. COLLECTION **17**
Overview 17
Knowing Who Knows 19
Collection Discipline 19
Collection Issues 20
Nuances of Open Source Collection 21
SECTION C. PROCESSING AND EXPLOITATION **23**
Overview 23
Analysis 23
Web-Site Authentication and Source Analysis 24
SECTION D. SEARCHING ANONYMOUSLY ON THE WEB **27**
Overview 27
Leaving a Footprint 28
Traffic analysis 28

Contact with others 29
SECTION E. PRODUCTION 29
Overview 29
Reports 29
Link Tables 31
Distance Learning 31
Expert Forums 32
SECTION F. DISSEMINATION AND EVALUATION 33
Overview 33
Dissemination Methods 34
Virtual Intelligence Community 34

CHAPTER IV 36
OSINT AND THE EMERGING FUTURE INTELLIGENCE ARCHITECTURE OF NATO 36
SECTION A. BLENDING OSINT INTO THE ALL-SOURCE PROCESS 36
Overview 36
Direction 38
Collection 39
Processing 41
Dissemination 42

APPENDIX A: GENERAL REFERENCE LINK TABLE 43
APPENDIX B: TRAINING LINK TABLE 45
APPENDIX C: CATEGORIES OF MISPERCEPTION AND BIAS 46
APPENDIX D: LIST OF ABBREVIATIONS 48
FEEDBACK 49

EXECUTIVE SUMMARY

COMMANDER'S OVERVIEW

Open Source Intelligence (OSINT) in Joint and Coalition Operations

Open Source Intelligence, or OSINT, is unclassified information that has been deliberately discovered, discriminated, distilled and disseminated to a select audience in order to address a specific question. It provides a very robust foundation for other intelligence disciplines. When applied in a systematic fashion, OSINT products can reduce the demands on classified intelligence collection resources by limiting requests for information only to those questions that cannot be answered by open sources.

Open information sources are not the exclusive domain of intelligence staffs. Intelligence should never seek to limit access to open sources. Rather, intelligence should facilitate the use of open sources by all staff elements that require access to relevant, reliable information. Intelligence staffs should concentrate on the application of proven intelligence processes to the exploitation of open sources to improve its all-source intelligence products. Familiarity with available open sources will place intelligence staffs in the position of guiding and advising other staff elements in their own exploitation of open sources.

Open Source Intelligence and Joint or Coalition Operations

OSINT is a vital component of NATO's future vision. Through its concentration upon unclassified open sources of information, OSINT provides the means with which to develop valid and reliable intelligence products that can be shared with non-NATO elements of international operations. Experience in the Balkans, and the increasing importance of the Partnership for Peace and Mediterranean Dialogue members in security dialogue, illustrates the need to develop information sources that enable broader engagement with these vital partners.

Private Sector Information Offerings

The Internet is now the default C4I architecture for virtually the entire world. The principle exceptions are most militaries and intelligence organizations. The Internet facilitates commerce, provides entertainment and supports ever increasing amounts of human interaction. To exclude the information flow carried by the Internet is to exclude the greatest emerging data source available. While the Internet is a source of much knowledge, all information gleaned from it must be assessed for its source, bias and reliability.

As a source of reliable information, the Internet must be approached with great caution. As a means with which to gain access to quality commercial sources of validated information, the Internet is unbeatable.

A vision of open source exploitation must not be limited exclusively to electronic sources. Traditional print, hardcopy images and other analog sources continue to provide a wealth of data of continuing relevance to NATO intelligence.

The Open Source Intelligence Cycle

As the range of NATO information needs varies depending upon mission requirements, it is virtually impossible to maintain a viable collection of open source materials that address all information needs instantly. The focus should be on the collection of sources, not information. With knowledge of relevant and reliable sources of open source information, an intelligence staff can quickly devote collection energy and analytical expertise to develop tailored OSINT products to the mission need.

OSINT and the Emerging Future Intelligence Architecture of NATO

OSINT is an essential building block for all intelligence disciplines. Open sources have always played a role in classified intelligence production. In the NATO context, a robust OSINT capability greatly increases the range of information sources available to intelligence staffs to address intelligence needs.

Nations are capable of tasking classified intelligence sources to address intelligence gaps. Lacking organic intelligence collection assets, NATO intelligence staffs are unable to task classified collection. Rather than immediately directed a Request For Information (RFI) to a national intelligence centre, a robust OSINT capability enables intelligence staffs to address many intelligence needs with internal resources.

While unable to replace classified intelligence production, OSINT is able to compliment an all-source intelligence production process with essential support including tip-offs, context, validation and cover for information sanitation.

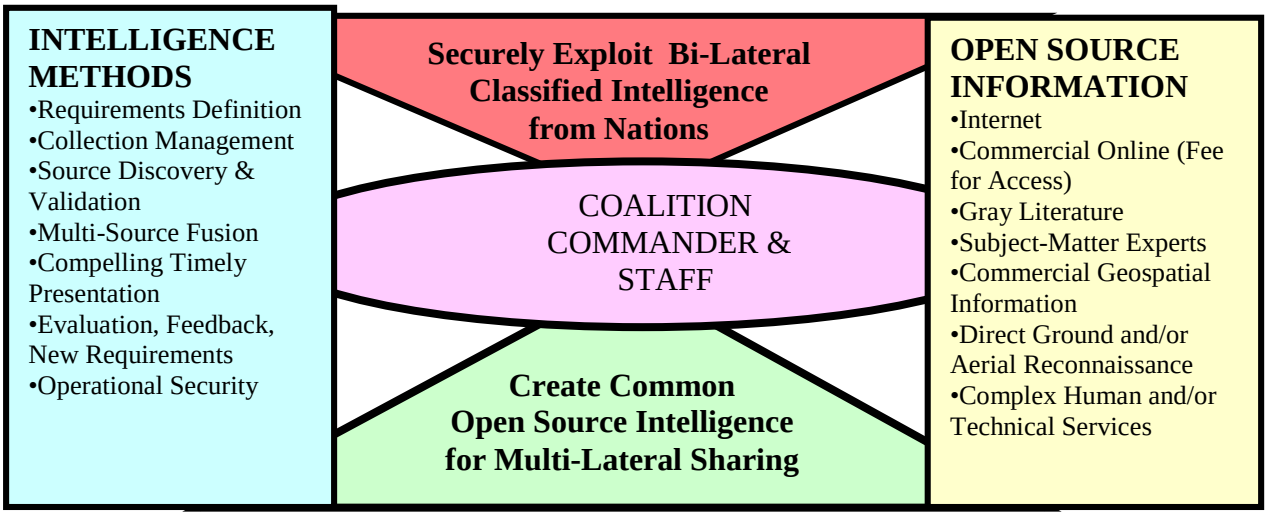
CHAPTER I
OPEN SOURCE INTELLIGENCE AND JOINT OR COALITION OPERATIONS

"OSINT is not a substitute for satellites, spies, or existing organic military and civilian intelligence capabilities. It is, however, a foundation—a very strong foundation—for planning and executing coalition operations across the spectrum from humanitarian assistance to total war. OSINT provides strategic historical and cultural insights; it provides operationally helpful information about infrastructure and current conditions; and it provides tactically vital commercial geospatial information that is not available from national capabilities. In coalition operations, OSINT is both the foundation for civil-military cooperation, and the framework for classified bilateral intelligence-sharing."

Introduction

OSINT is distinct from academic, business or journalistic research in that it represents the application of the proven process of national intelligence to a global diversity of sources, with the intent of producing *tailored* intelligence for the commander. OSINT is also unique, within a coalition operations context, in that it simultaneously provides a multi-lateral foundation for establishing a common view of the shared Area of Operations (AOO), while also providing a context within which a wide-variety of bi-lateral classified intelligence sharing arrangements can be exploited. Figure 1 illustrates these relationships.

Figure 1 - Relationship between Open Source and Classified Information Operations



OSINT is valuable to NATO member nations and to individual Partner nations in that it can be used to provide a common understanding of the AOO across all elements of its military forces and its civilian and non-governmental organization (NGO) counterparts. Elements of the forces not authorized access to the full range of classified information, often including such vital components, as military police, logistics elements, engineers, and the public affairs staff, can be made more effective through the utilization of tailored OSINT. At the same time, external parties with whom coordination is critical, but who are also not authorized access to classified information, can receive tailored OSINT that is helpful to a shared understanding of the AOO and the challenges facing the coalition and all its elements. Figure 2 illustrates this idea.

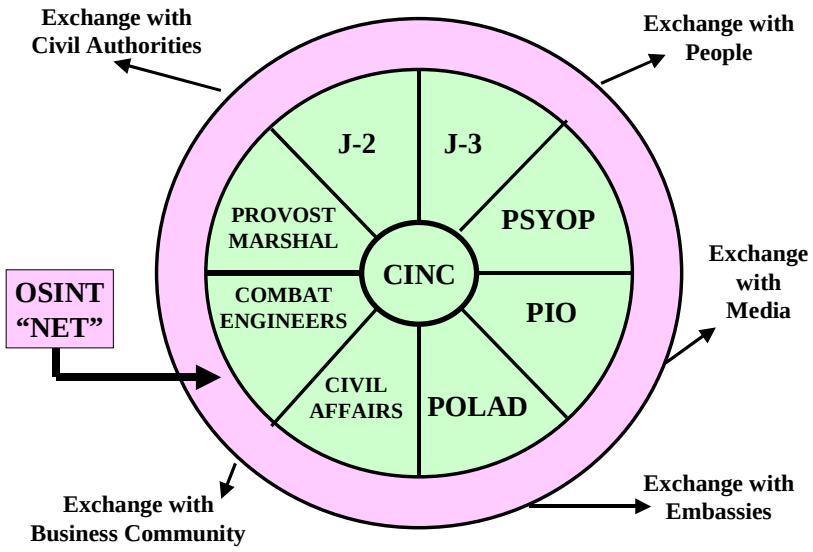


Figure 2 - Utility of OSINT Net for Internal and External Information Exchanges

Definitions

There are four distinct categories of open information and intelligence.

Open Source Data (OSD). Data is the raw print, broadcast, oral debriefing or other form of information from a primary source. It can be a photograph, a tape recording, a commercial satellite image, or a personal letter from an individual.

Open Source Information (OSIF). OSIF is comprised of data that can be put together, generally by an editorial process that provides some filtering and validation as well as presentation management. OSIF is *generic* information that is usually *widely disseminated*. Newspapers, books, broadcast, and general daily reports are part of the OSIF world.

Open Source Intelligence (OSINT). OSINT is information that has been deliberately discovered, discriminated, distilled, and disseminated to a *select*

audience, generally the commander and their immediate staff, in order to address a *specific* question. OSINT, in other words, applies the proven process of intelligence to the broad diversity of open sources of information, and *creates intelligence*.

Validated OSINT (OSINT-V). OSINT-V is information to which a very high degree of certainty can be attributed. It can be produced by an all-source intelligence professional, with access to classified intelligence sources, whether working for a nation or for a coalition staff. It can also come from an assured open source to which no question can be raised concerning its validity (images of an aircraft arriving at an airport that are broadcast over the media).

21st Century Information Operations

OSINT is an essential contextual and foundation element for classified intelligence operations. Overt human sources can help target and validate clandestine human intelligence (HUMINT) sources. Overt broadcast information can be used to better understand covertly collected signals intelligence (SIGINT). Commercial geospatial information, especially wide-area surveillance imagery, can be used to significantly enhance the value of the more narrowly focused covert imagery intelligence (IMINT) capabilities. OSINT can also make contributions to the emerging discipline of Measurements and Signatures Intelligence (MASINT), to Counter-intelligence (CI), and to Operations Security (OPSEC).

OSINT is the major new "force" in 21st Century Information Operations (IO). OSINT is not "new" in that Nations and organizations have always understood the value of legal travelers, direct observation, structured reading, and legal purchases of information services. What *is* new about OSINT is the confluence of three distinct trends: first, the proliferation of the Internet as a tool for disseminating and sharing overt information; second, the consequent and related "information explosion" in which published knowledge is growing exponentially; and third, the collapse of many formerly denied areas.

OSINT is important to coalition commanders and their staffs for another reason: emerging threats, and the lower end of the spectrum of conflict, increasingly demand out-of-area operations and engagement in operations for which classified intelligence support is not readily available. Out of area operations such as humanitarian assistance and disaster relief operations in the countries of Africa or elsewhere along the NATO periphery, are all characterized by complex information needs related to infrastructure, demographics, health, and other matters not traditionally addressed by classified intelligence collection operations.

OSINT is vital to government operations, and especially to coalition operations, for one additional reason: the changing nature of command & control in the 21st Century. In the past, nations and even coalitions relied heavily on a top-down "chain of command" that relied on closed sources to direct generally unilateral actions with short-term time frames. Today, as non-governmental organizations come to the fore and are often the predominant factors in many of the operations that the military must support, the dynamics of both command & control and information have changed.

Within NATO, operations must be planned and executed in a multi-cultural fashion, with bottom-up consensus often being the most effective means of arriving at sustainable decisions. This is particularly true with the vital role played by non-NATO troop contributing nations. Under these circumstances, a common view of the

operating area, formed with the help of validated OSINT is often the most effective means of delivering decision-support.

The remainder of this manual will discuss private sector information offerings, the open source intelligence cycle, and the integration of OSINT into the NATO and prospective PfP coalition operations. OSINT will be a core element of the NATO Future Intelligence Architecture.

Special Note on Operational Security

The most common objection to the use of open sources of information, apart from the general lack of knowledge and funding with which to exploit open sources, relates to Operational Security (OPSEC). This topic is fully discussed within Chapter III. The Open Source Intelligence Cycle makes full provision for OPSEC at every stage, and ample methods exist to conceal the commander's intent, the source of the inquiry, and other sensitive aspects of open source exploitation.

CHAPTER II
PRIVATE SECTOR INFORMATION OFFERINGS

The four pillars to an OSINT strategy are sources, software, services and analysis. The private sector can address all four to some degree. Analysis is the key enabling skill that is essential to the successful integration of OSINT into an all-source intelligence product. While some analysis of open sources can and should be acquired from private sources, those analytical skills necessary to integrate open source derived intelligence must be grown and nurtured within intelligence staffs. Analysis will be discussed further in Chapter III. This chapter is intended to expose the wider audience to the range of OSINT-related products that the private sector are optimized to provide.

SECTION A. SOURCES

Traditional Media Sources





To many, media sources were the only open sources that were familiar prior to the onset of the Internet. These include traditional foreign print and broadcast media, radio and TV as well as the current array of electronically available products. For current intelligence purposes, media sources remain the core capability necessary for an OSINT effort and are available from a variety of providers. Direct wire-service feeds are available. Commercial online premium sources discussed below all provide an array of media sources on a fee for service basis.

While not private sector information providers, the U.S. Foreign Broadcast Information Service (FBIS) and the British Broadcasting Corporation (BBC) Monitoring Service each provide excellent near real-time translation of foreign media sources. In addition, an array of media analysis products supplement the direct listing of foreign broadcasts and provide useful insight into the general character of foreign media reporting on particular issues.

Internet

The Internet has, since 1994, literally exploded on to the world scene and changed forever the manner in which individuals might carry out global research. According to Dr. Vinton Cerf, acknowledged by many to be one of the founders of the Internet, it will grow from 400 million users in November 2000, to an estimated 3.5 billion users by the year 2015.

Apart from this exponential increase in the number of human beings using the Internet, other experts project a double or triple order of magnitude increase in the use of the Internet to connect devices, from geospatial locators in vehicles, to temperature detectors in soda machines, to usage monitors in doorways. The Internet is at the very beginning of its development as a global grid of enormous value to coalition operators, logisticians, and intelligence professionals.



Figure 3 - Internet users by continent (1999)

The Internet has been over-sold in the past. A study by the Community Open Source Program Office (COSPO) within the U.S. Intelligence Community concluded in 1994 that the Internet only contained roughly 450 useful substantive sites, and that 99% of the Internet was not content of intelligence value, but rather pornography, opinion, and advertising. This earlier evaluation of the intelligence potential of the Internet no longer reflects the extensive content that is now available. Some suggest that over 250,000 databases are now available within the "deep web", a great many of which are of potential intelligence value.

While the Internet has grown substantially in value since 1994, the intelligence professional must be very cautious about both over-reliance on the Internet, and about the source bias of materials found there. In general, Internet sources are rarely dated, formatted, paginated, edited, filtered, or stable, even when addressing substantive topics.

The Internet is an "easy out" for operators and other consumers of intelligence. It is an attractive option for commanders and staff in a hurry. If intelligence professionals do not demonstrate that they monitor and exploit the Internet, and/or if intelligence professionals make it too difficult for consumers to obtain usable all-source intelligence, the Internet represents a "threat" to the existing intelligence process. Increasingly, intelligence professionals must act to place information that is widely available on the Internet into its proper context – either confirming its validity or disputing the information based on classified collateral reporting.

In general, the Internet today provides two benefits to the coalition professional: first, as a means of rapidly communicating with counterparts around the world, primarily to exchange unclassified information and professional insights; and second, as a means of rapidly accessing both free and premium (fee paid for access) information sources. However, the Internet also has its dangers. Electronic mail and attached documents comprise a permanent record in cyber-space, and the sender has little control over subsequent dissemination and exploitation.

OSINT Professional Note: A number of advanced search tools are available that complement the variety of search engines that are freely available on the Internet. OSINT managers should remain abreast of developments in the field of Internet tools and integrate appropriate tools, as they become available, into their OSINT process. An example, its basic form available free or in an advanced version at a small cost, is a meta-search engine that combines the best features of multiple search engines, while also permitting subsequent searches for new information (remembering what has already been seen). Download this program from www.copernic.com.

Commercial Online Premium Sources

There are numerous commercial online premium sources, that is, sources that charge either a subscription fee or a usage fee for access to their information. It is essential that every professional understand the availability and the value of commercial online premium sources. They represent decades worth of editorial selection,

authentication, formatting, indexing, abstracting, and presentation management. In general, source material obtained through a commercial online premium service has been created by a reputable commercial enterprise subject to scrutiny and the judgment of the marketplace. In Figure 4, we discuss the three best known to governments and corporations. There are many others, some unique to Europe or Asia. Each professional is urged to consult his or her librarian or his or her OSINT collection manager to gain a better understanding of what their options are for high-quality commercial information relevant to their action responsibilities.

In general, and in part because of the high cost of mistakes or unnecessary retrievals, all commercial online premium services should be searched by those staff with sufficient training on the database and a thorough understanding of its pricing structure. Even commands with flat-fee pricing should be aware that their next contract will be increased in price based on actual usage during the current flat-fee period. Alternatively, an option is to gain access to commercial sources via the services of a professional librarian or commercial information broker. Most professional information brokers, such as those belonging to the Association of Independent Information Brokers (AIIB), specialize in either LEXIS-NEXIS or DIALOG. There are distinct advantages in contracting a searcher who has detailed familiarity with the very arcane search command characteristics of these two services. In the case of Factiva this is less vital but can still make a big difference in both the success of the searchers, and the cost of the searches.

FACTIVA	LEXIS-NEXIS	DIALOG
www.factiva.com	www.lexis-nexis.com	www.dialog.com
Best web-based user interface, easiest means of searching all available publications. Archive of publications varies but typically provides several years worth of historical file. Includes Jane's Information Group material as well as BBC transcripts. Does not include FBIS information.	Two separate channels, one focused on legal sources including public records (primarily in the United States but very helpful in tracing real estate, aircraft, and water craft including international ships), the other focused on news sources but offering archive access, i.e. ability to reach back several years or more on any topic.	A very large collection of various commercial offerings that can be searched "by the file". Especially valuable for access to conference proceedings, academic and policy journals, dissertations, book reviews, and the Social Science Citation Index (SSCI). The latter is ideal for finding and ranking individual experts, to include identification of their official address.
Flat fee or actual cost pricing.	Flat fee, actual cost, or pay as you go credit card pricing.	Flat fee, actual cost, or pay as you go credit card pricing.

Figure 4 - Leading Commercial Online Premium Sources

OSINT Professional Note: Always ask for search results in electronic form, these files can more easily be shared. Copy the results into a Word document. Add pagination. Add a title page and a blank table of contents page. Sort the items into larger categories (e.g. Political, Military, Economic) and label the categories as "Heading 1". Then go through the document label each individual headline as "Heading 2". These headings are choices in the style bar at the upper left that generally says "Normal". Finally, go to the Table of Contents and use the Insert, Index and Tables, Table of Contents choices to insert a table of contents. If desired, use the Replace function to find and make bold all of the original search terms.

Other Forms of Commercial Online Information

There is a vast range of commercial sources available through direct subscription, both on the Internet and in the form of hard copy or CD-ROM publications. Table 1 below identifies just a few sources of common interest to military commanders and their staff. There are many more than those listed here. SACLANT has undertaken to develop and maintain a common NATO inventory of open sources and access points to which RFIs can be directed. This can be found on MCCIS at www.saclant.nato.int/intel. Work continues to progress on a concept of operations for establishing broad NATO access to such sources at the most competitive prices possible.

Source Type or Function	Source Name and URL
Broadcast Monitoring	BBC Monitoring http://news.monitor.bbc.co.uk/
Broadcast Monitoring	FBIS/NTIS World News Connection http://wnc.fedworld.gov/ntis/home.html
Commercial Imagery	Autometric http://www.autometric.com/AUTO/SERVICES/GIS
Current Awareness (Conferences)	British Library Proceedings http://www.bl.uk/services/bsds/dsc/infoserv.html#inside_conf
Current Awareness (Journals)	ISI Current Contents http://www.isinet.com/
Current Awareness (Regional)	Oxford Analytica http://www.oxan.com/
Defense Monitoring	Janes Information Group http://www.janes.com/geopol/geoset.html
Defense Monitoring	Periscope http://www.periscope1.com
Defense Monitoring (NATO)	Orders of Battle Inc. http://orbat.com
Directories of Experts	Gale Research http://www.gale.com/
Foreign Affairs Discussions	Columbia U. Int'l Affairs Online www.ciaonet.org
Foreign Affairs Monitoring	Country Watch.com www.countrywatch.com
Global Risk Monitoring	Political Risk Service (Country Studies) www.prsgroup.com
Maps & Charts	East View Cartographic http://www.cartographic.com

Table 1 - Examples of specialized commercial information

Grey Literature

Grey literature is that information that is both legally and ethically available, but only from specialized channels or through direct local access. It is generally understood as that information whose distribution is not controlled by commercial publishers, and/or that information that is not published, distributed, catalogued or acquired through commercial booksellers and subscription agencies. Grey literature includes working

papers, pre-prints, technical reports and technical standards documents, dissertations, data sets, and commercial imagery. Producers of grey literature include: non-profit and educational organizations; commercial enterprises creating documents for internal use as well as for clients and suppliers; local, state, and national government agencies producing materials for internal use as well as for citizens and vendors, and; a wide variety of informal and formal associations, societies, and clubs. Examples include university yearbooks, yacht club registries, corporate trip reports, and personal notes from public events that are posted to a public bulletin board.

Overt Human Experts and Observers

The ultimate open source is a human expert or human observer with direct experience. In many places of the world, Africa, for example, it is not possible to obtain published information on specific locations or conditions. For many topics, even those with great quantities of published information, it is not possible to find exactly what is needed even when the time and money is available to collect, process, and analyze all available published information. The human expert is often the most efficient and the most inexpensive means of creating new open source intelligence that is responsive to a specific requirement from the commander or his staff.

The identification and interviewing of those with direct on-the-ground experience is also a valuable means of ascertaining "ground truth." It merits comment that official communications from organizations, and most media reporting, tend to rely on second-hand reports. Unless the information is meticulously sourced and from a very trusted source, expert judgment or observation more often than not it will be less reliable than direct human expert judgment or observation.



OSINT Professional Note: There are essentially four ways to get to expert humans. The most effective means is through citation analysis using the *Social Science Citation Index* (SSCI) or the *Science Citation Index* (SCI). These can both be accessed at www.isinet.com/isi. This generally requires a specialist searcher with access to DIALOG for the SSCI or to the Scientific and Technical Network (STN) for the SCI. The second means is through professional associations such as listed in the *International Directory of Associations* published by Gale Research, or as found through a copernic.com search of the Internet. The third means is by doing a Factiva.com search and identifying experts or "talking heads" that have been quoted in the media on that topic. Last, and often the least efficient, is through a labor-intensive series of telephone calls to various known government agencies or official points of contact. As a general rule, it is best to do a comprehensive professional search for international experts with the most current knowledge, rather than relying on the in-house focal points or whomever might be casually known to in-house points of contact.

Commercial Imagery

The commercial imagery industry continues to mature with the launching in recent years of a number of satellites that offer militarily significant capabilities. One-meter

resolution electro-optical imagery available to the private sector is not only possible now but also likely to be *de rigueur* in the future. Table 2 illustrates some of the military applications of 1-m commercial imagery. By 2003, at least eleven private companies expect to have high-resolution commercial remote sensing satellites in orbit. Their products will be available to whoever has a credit card. While this will bring new capabilities to friend and foe alike, commercial imagery provides unique opportunities for NATO as well. Unbridled by security constraints, which limit the use of imagery derived from military satellites, commercial imagery acquired by NATO can be freely distributed within the constraints of copyright agreements with the original provider. This provides a host of options regarding cooperation with broader coalition partners who do not have access to NATO classified information.

Target *(note a)*	**Detection** *(note b)*	**General ID** *(note c)*	**Precise ID** *(note d)*	**Description** *(note e)*	**Technical Analysis**
Troop units	**6.0**	**2.0**	**1.20**	**0.30**	**0.150**
Vehicles	**1.5**	**0.6**	**0.30**	**0.06**	**0.045**
Aircraft	**4.5**	**1.5**	**1.00**	**0.15**	**0.045**
Airfield facilities	**6.0**	**4.5**	**3.00**	**0.30**	**0.150**
Nuclear weapons components	**2.5**	**1.5**	**0.30**	**0.03**	**0.015**
Missile sites (SSM/SAM)	**3.0**	**1.5**	**0.60**	**0.30**	**0.045**
Rockets and artillery	**1.0**	**0.6**	**0.15**	**0.05**	**0.045**
Surface ships	**7.5-15.0**	**4.5**	**0.60**	**0.30**	**0.045**
Surfaced submarines	**7.5-30.0**	**4.5-6.0**	**1.50**	**1.00**	**0.030**
Roads	**6.0-9.0**	**6.0**	**1.80**	**0.60**	**0.400**
Bridges	**6.0**	**4.5**	**1.50**	**1.0**	**0.300**
Communications					
Radar	**3.0**	**1.0**	**0.30**	**0.15**	**0.015**
Radio	**3.0**	**1.5**	**0.30**	**0.15**	**0.015**
Command and control HQs	**3.0**	**1.5**	**1.00**	**0.15**	**0.090**
Supply dumps	**1.5-3.0**	**0.6**	**0.30**	**0.03**	**0.030**
Land minefields	**3.0-9.0**	**6.0**	**1.00**	**0.30**	**--**
Urban areas	**60.0**	**30.0**	**3.00**	**3.00**	**0.750**
Coasts, landing beaches	**15.0-30.0**	**4.5**	**3.00**	**1.50**	**0.150**
Ports and harbors	**30.0**	**15.0**	**6.00**	**3.00**	**0.300**
Railroad yards and shops	**15.0-30.0**	**15.0**	**6.00**	**1.50**	**0.400**
Terrain	**--**	**90.0**	**4.50**	**1.50**	**0.750**

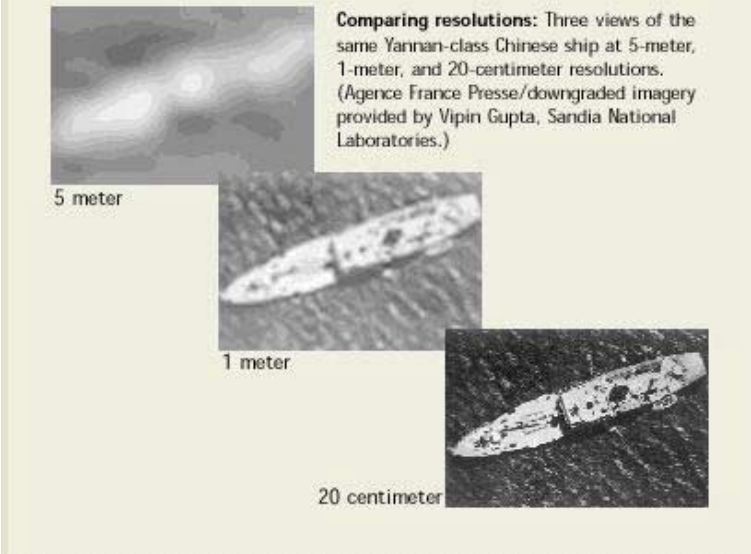
Notes:

a. The table indicates the minimum resolution in meters at which the target can be detected, identified, described, or analyzed. No source specifies which definition of resolution (pixel-size or white-dot) is used, but the table is internally consistent.
b. Detection: location of a class of units, object, or activity of military interest.
c. General identification: determination of general target type.
d. Precise identification: discrimination within a target type of known types.
e. Description: size/dimension, configuration/layout, components construction, equipment count, etc.
f. Technical Analysis: detailed analysis of specific equipment.

Table 2 - Approximate Ground Resolution in Metres for Target Detection, Identification, Description and Analysis

Source: Yahya A. Dehqanzada and Ann M. Florini. *Secrets for Sale: How Commercial Satellite Imagery Will Change the World*. Washington D.C.: Carnegie Endowment for International Peace, 2000.

The individual satellites are currently limited by poor revisit times to specific targets. This factor is mitigated by the growing "virtual constellation" of commercial remote sensing satellites that is comprised of the collective resources of all of the available private companies. The Western European Union (WEU) satellite center has grown its capability through the concept of exploitation of all available commercial resources rather than restricting to merely European sources.



Comparing resolutions: Three views of the same Yannan-class Chinese ship at 5-meter, 1-meter, and 20-centimeter resolutions. (Agence France Presse/downgraded imagery provided by Vipin Gupta, Sandia National Laboratories.)

Figure 5 - Comparative imagery resolutions

In addition to electro-optical sensors, Synthetic Aperture Radar (SAR) imagery capability is improving significantly. SAR imagery relies upon the analysis of a signal transmitted in the microwave part of the electromagnetic spectrum and the interpretation of its return signal. Unlike electro-optical systems, these sensors are not limited to daylight operations. Because they have an active sensor, they can image a target in day or night, in any weather, through clouds and smoke.

While current systems are capable of 8-meter resolution, the next few years will see commercial SAR satellites providing 1-meter resolution. These systems will be able to provide a dependable source of militarily significant commercial imagery to NATO forces as well as to our adversaries.

A number of NATO nations purchase commercial imagery to support their own national imagery requirements. In many cases, these images can be redistributed freely. While NATO commands are able to purchase commercial imagery themselves, national sources of imagery should be consulted, as part of any collection effort, to ensure that commercial imagery needs cannot be addressed through existing sources.

The "virtual constellation" of commercial remote sensing satellites will ultimately be able to provide a target revisit schedule that will increase its reliability as a source of imagery. Until that time, the vast archive of commercial remote sensing images remains a rich source of historical data that can be acquired fast and at low cost. Historical data is optimized for mission planning, mapping and humanitarian support operations when detailed knowledge of infrastructure is essential.

Defining Source Access Requirements (Dangers of Pay-per-View)

It is a relatively easy endeavor to identify private information sources that can support the information needs of an OSINT programme. With the proliferation of restricted and open access Intranets, there are great pressures to place all information acquired onto web-based dissemination systems.

While single copy licenses to information

sources are typically attractively priced, multiple user licenses increase in price. License costs are generally a factor of the number of users that have access to the information. To place information directly onto servers without the knowledge and consent of the information provider is a violation of copyright laws.

An option to reduce costs is to determine the information needs of the organization based on communities of interests. Some information is required by all staff and merits a general site license. Other information is of interest to a more restricted audience. Lloyd's shipping data, for example, may be of general interest to a wider audience but of job specific interest to a select group of analysts. The purchase of a limited site license and the use of restricted access within the Command's Intranet will greatly reduce license costs yet still provide the information in the most effective manner. Finally, ad hoc information requirements may be addressed with the acquisition of single copies of key information sources.

As a general rule, there are few information sources that are required by all members of a staff. Restricting access to some sources will increase the range of open sources that are available for purchase within an organization's OSINT budget. Careful planning and the identification of the logical communities of interest for individual open sources is a reasonable approach to manage scarce resources.

SECTION B. SOFTWARE

Software Hierarchy

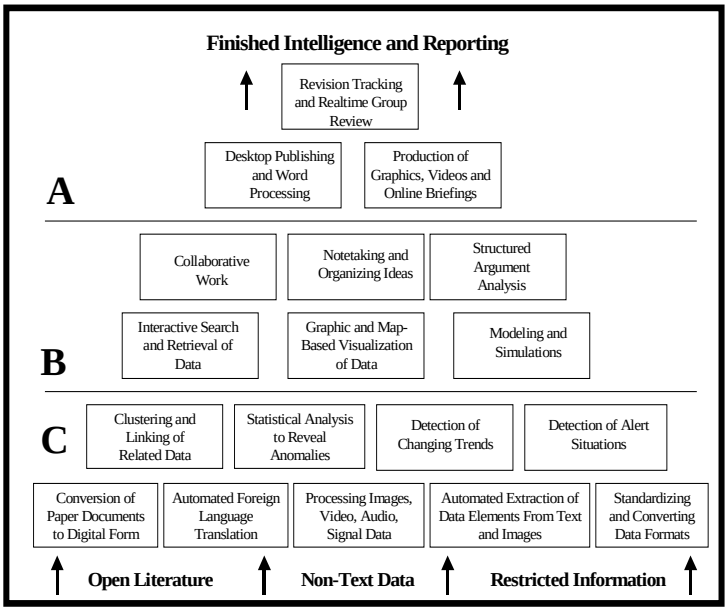


Figure 6 - OSINT Software Hierarchy

Above is an illustration of the eighteen distinct software functionalities that have been identified as being necessary for the optimal processing of open sources of information by any analyst—these would comprise the desktop "toolkit."

Section A functionalities include publishing and production management functionalities. Section B functionalities combine

collaborative work tools with data visualization and manipulation tools with thinking tools: modeling and simulation and structured argument analysis. Section C functionalities combine tools for the automated pre-processing of data once it is digital, and with tools for converting hard copy and multi-lingual or multi-media information into a single digital standard.

Unfortunately, the state of the software industry in general, and of desktop software in particular, is such that today it is not possible to integrate all of these functionalities at an affordable cost. A major obstacle to progress is the existing industry practice of concealing and constantly changing Application Program Interfaces (API). This means that third party software producers desiring to have their offerings work with another major product, must undertake lengthy and often expensive negotiations in order to be shown the proprietary API. Software today is still not "plug and play", and it is unlikely to become fully intergratable "out of the box" until standards of stability and transparency for API are established.

Having said this, it is possible to identify several software packages of some value to the open source intelligence analyst or the action officer working with open source intelligence.

SECTION C. SERVICES

Collection Services

Collection services include online collection (searchers that specialize in Internet, deep web and premium commercial online source exploitation); off-line grey literature or document acquisition; telephone surveys and electoral or other forms of polling; private investigations and human intervention services ("boots on the ground"); and aerial surveillance or reconnaissance services.

Processing Services

Processing services include data conversion from hard-copy or analog to digital, indexing and abstracting of hard-copy or soft-copy textual data or images, interpretation and annotation of imagery or signals, database construction and stuffing, and complex modeling & simulation projects with the best ones including geospatial and time-based visualizations.

When integrated with well-planned open source collection and the right analytical expertise, complex processing services can yield substantial dividends by compressing large amounts of data into manageable tailored products that address specific intelligence requirements.

Analysis & Production Services

A wide variety of commercial and academic organizations offer diverse analysis and production services. As a general rule, the best value is found through the hiring of single individual experts with no overhead, rather than through broad contracts with organizations that then adds a substantial fee for their considerable overhead expenses.

The very best value results when niche collection, niche processing, and niche analysis services can be "mixed and matched" to obtain precisely the desired results. The very worst value comes when an organization is hired because of a convenient contract, they do not have a niche expert, and choose to dedicate an

analyst that does not bring sufficient experience or skill to the task.

Industry leaders can best be identified with reference to citation analysis and familiarity with their product set. This is best accomplished through the identification of other organizations with similar intelligence problems and exchanging information concerning those validated information vendors that they employ. Web-site analysis is another tool, which can be applied to vet the capabilities of a potential information vendor.

Services Examples

Data Conversion	ACS Defense www.acsdefense.com
Database Construction & Stuffing	ORACLE www.oracle.com
Document Acquisition	British Library Document Centre http://www.bl.uk/services/bsds/dsc/
Human Intervention	The Arkin Group www.thearkingroup.com
Imagery Interpretation & Annotation	Boeing Autometric www.autometric.com
Indexing & Abstracting	Access International http://www.accessinn.com/
International Studies Analysis	Monterey Institute of International Studies www.miis.edu
Modeling & Simulation	Boeing Autometric www.autometric.com
Online Collection	Association of Independent Information Professionals www.aiip.org
Open Source Intelligence Portal (meta-service)	Open Source Solutions Inc. www.oss.net
Private Investigation	Intelynx (Geneva) www.intelynx.ch
Scientific & Technical Analysis	CENTRA www.centratechnology.com
Signals Processing	Zeta Associates Incorporated www.zai.com
Telephone Surveys (Primary Research)	Risa Sacks & Associates www.rsacksinfo.com

Table 3 - OSINT Related Services

As a general rule, there are no "portal" companies that serve as honest brokers for helping governments "mix and match" best in class niche providers at the most economical cost.

CHAPTER III
THE OPEN SOURCE INTELLIGENCE CYCLE

SECTION A. OSINT PLANNING AND DIRECTION

Overview

Whether one is going after open source data, information, or intelligence, there is a proven process of intelligence, the intelligence cycle that will yield good value when applied. The open source intelligence process is about discovery, discrimination, distillation, and dissemination—the 4 Ds (Figure 7). This analytical approach is applied to the traditional single source intelligence cycle. A good understanding of the open source intelligence cycle makes it possible to access and harness private sector knowledge using only legal and ethical means, generally at a very low cost in comparison to covert technical or clandestine human collection. Since many requirements that are urgent for the commander and their staff may not qualify for nor be appropriate for secret collection methods, the open source intelligence cycle is in fact *vital* to NATO planning and operations. As will be seen in the following discussion, OSINT is an emerging discipline and the emphasis will often be on informal coordination rather than formal tasking.

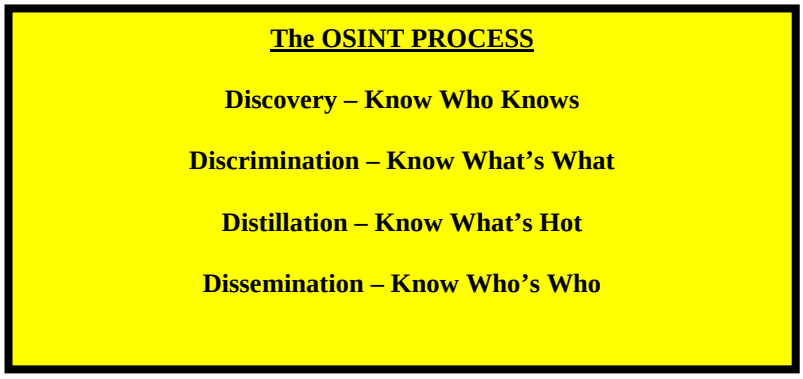


Figure 7 - The OSINT Process

Organizations and Responsibilities

The commander is ultimately responsible for establishing the Essential Elements of Information (EEI) and for applying the resources necessary to satisfy them. Open source intelligence is *not* necessarily the responsibility of, or available from, national-level intelligence organizations. While the intelligence staff typically acts as the staff principal for OSINT activities, other staffs are frequently well placed to both collect open sources and to facilitate the further development of sources on behalf of the Command. The subordinate commanders for Civil Affairs, Public Relations, Military Police, and Combat Engineering may often be the best channels for seeking out OSINT, and can comprise an informal advisory council to the commander.

OSINT sources include, but are not restricted to:

- **National-Level Intelligence Organizations**. Although they are not responsible for satisfying the commander's needs for OSINT, national-level intelligence organizations may have relevant open source information that can be provided. Some countries, such as The Netherlands, United Kingdom, Denmark and Norway, are exceptionally competent in this area and have fully integrated OSINT into their all-source collection and production environments. Others may have selected units that can be called upon, but have not yet mastered this discipline.

- **Diplomatic Missions**. The established diplomatic missions of the various member nations are often the best source of OSINT, at little cost, if they are approached by one of their nationals acting in an official capacity on behalf of the commander. Such missions are under no direct obligation to respond, but informal coordination may yield good results.

- **Chambers of Commerce**. Many of the member nations have Chambers of Commerce and these often have established small communities that bring the general managers and key business executives from their national firms in any given country together. On an informal basis, with clear disclosure of the commander's interest, useful OSINT may be acquired. This is particularly true in deployed areas.

- **Non-Governmental Organizations**. The International Committee of the Red Cross (ICRC), Doctors Without Borders, and the many elements of the United Nations as well as the many international relief and charity organizations, have deep direct knowledge that can be drawn upon through informal coordination.

- **Religious Organizations**. Many Non-Article 5 Operations have very substantial human mass migration and ethnic conflict aspects as witnessed during Operation Allied Force. These issues are often best understood by religious organizations. Organizations such as The Papal Nuncio and the local Opus Dei, the B'nai Brith, the Islamic World Foundation, and other equivalent religious organizations are an essential source of overt information and expert perceptions

Requirements Definition

The greatest challenge for the commander will be the establishment and maintenance of a rigorous and disciplined process for defining the requirements to be addressed through open sources. The common attitudes of "tell me everything about everything" or "if I have to tell you what I need to know you are not doing your job" represent unworkable direction.

Commanders and their staff must carefully evaluate the specific information needs in the context of their concerns and their plans and intentions, and they must articulate, in the narrowest possible way, precisely what they want to know and why. The commander's operational intent is as vital to the intelligence professional as it is to the operations professional. Only by understanding the context and direction of the commander's requirements, can a truly focused and flexible collection effort be undertaken.

OSINT is the most fundamental and fastest means of satisfying basic informational

needs, including needs for historical background, current context and general geospatial information. Each commander should distinguish between their tailored intelligence requirements in support of their future planning and the basic information requirements that will permit operational and logistics and other special staff planning (e.g. Civil Affairs) to go forward. OSINT is highly relevant to both kinds of intelligence support.

Evaluation and Feedback

Planning and direction is a continuous process. The commander and their staff must digest, evaluate, *and provide feedback on* all received intelligence, whether open or classified. As open source intelligence is received and reviewed, it must be shared with staff principals and subordinate commanders, evaluated, and the results of the evaluation passed directly to the staff element responsible for coordinating OSINT support to the commander.

SECTION B. COLLECTION

Overview

The heart of intelligence collection is research – it is the matching of validated intelligence requirements to available sources with the aim of producing a product that answers a valid need. Once an intelligence need has been identified, open sources should be reviewed by intelligence staffs to determine if that intelligence need can be satisfied through those resources organic to the intelligence staffs, those resources that the staff can access, if an RFI to nations is required, or if a combination of these approaches is required.

Collection requires the translation of an intelligence need into an intelligence requirement – an action plan to answer that need. A collection strategy is developed to tap available sources. Optimal sources are selected and the information is collected. This generic collection approach is equally applicable to classified sources as it is to open sources.

In the NATO context, OSINT is a contributing source to an all-source intelligence effort. Open sources are used to compliment the existing classified intelligence and can be collected on a specific area. OSINT-derived products are created to answer a specific intelligence need to which open sources are best optimized. While RFIs from intelligence users typically generate collection efforts, Table 4 illustrates the three types of producer generated intelligence collection and production requirements.

These three categories outline the way in which an internally directed OSINT

Analyst-driven	**Based on knowledge of customer and issues**
Events-driven	**In response to time-sensitive relevant events**
Scheduled	**Periodic activities to document and update target status**

Table 4: Types of Producer-Generated Intelligence Collection and Production Requirements

Source: Arthur S. Hulnick. "The Intelligence Producer-Policy Consumer Linkage: A Theoretical Approach." Intelligence and National Security, Vol. 1,No. 2, (May 1986)

collection strategy should be developed. Only those products that support the intelligence staff's mission should be produced. The range of open information that is available both freely and commercially will swamp the analytical capacity of any intelligence staff regardless of size. Therefore, effective management must include the avoidance of production without a specific purpose. While not advocating a "make work" approach to intelligence, producer-generated collection builds skills, evaluates sources and increases capabilities necessary to address future RFIs and production requirements.

An analyst is often best placed to determine what product is required to address the past needs of the intelligence user. Proactive collection and management to make effective use of emerging information should be encouraged. This could include the tailoring of a newly available public report that addresses an established intelligence need into a format of use to an intelligence user.

Rapidly changing events can drive the production of new products. A military coup or an environmental crisis could presage increased NATO interest in an area of non-traditional interest. In the absence of national intelligence production shared with NATO, open source collection may be the best means with which to begin to build an intelligence picture for the command.

Less dramatic changes to the international environment may also require open source collection. Seasonal changes in a particular region may lead to population migration. These periods are known well in advance and lend themselves to scheduled production of necessary intelligence products.

Chapter II reviewed private sector information offerings. Chapter III focuses on the methods to be applied by any NATO unit to exploit those offerings, while not recommending any specific source, software, or service. What is important is that every NATO unit is conscious of the overall process, the alternative means for obtaining and exploiting OSINT, and the value of OSINT as part of the all-source intelligence cycle. Figure 8 below is provided a high-level view of the elements of the OSINT collection process.

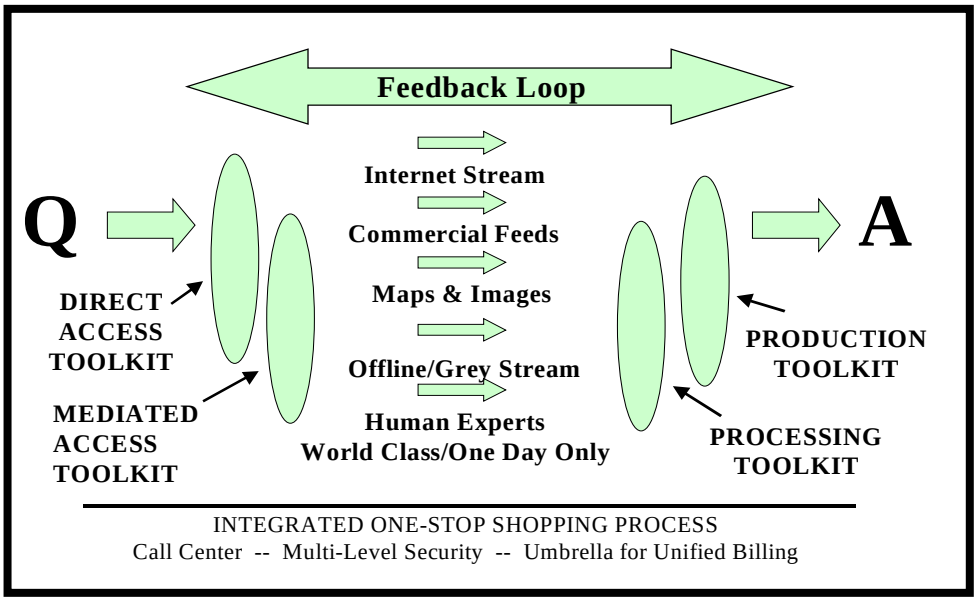


Figure 8 - OSINT Collection Process

Knowing Who Knows

During periods of stability as well as crisis, it is incumbent upon intelligence staffs to establish and nurture sources that will help satisfy information requirements. It is vital that the OSINT professional, known in some governments as Open Source Officers (OSO), focuses initially on "knowing who knows" – the ability to rapidly identify subject matter experts on topics of direct relevance to the commander's mission and to seek information from them.

An approach favoured by some is the concept of collecting sources not information. While the array of available open sources is staggering, the ability to focus collection quickly on an emerging issue of intelligence interest is the key capability. Rather than having a stale open source product to draw upon, the ability to rapidly direct collection on an issue, identify the leading experts on the field and either draw upon their most recent work or contact them directly is the most effective use of an OSINT capability.

Therefore, a standing collection priority should include a preliminary inventory of subject-matter experts (SME) within the parent commands and its subordinate, adjacent, and higher commands, but should then extend further, throughout the parent government and into the national private sector. The business community with its international chambers of commerce, the academic community with its various professional associations, and the non-governmental organizations including the peace institutes resident in many countries, are all vital points of reference.

The command OSO is, in essence, an information attaché to each of these elements, and must always act with the highest standards of overt decorum and propriety. This must include a firm grasp of both the private sector's rights and obligations with respect to copyright and the protection of intellectual property, and NATO's concerns with regard to OPSEC.

Collection Discipline

There is no faster way for an OSO to lose his commander's respect than to try to do too much, and end up taking too long to produce simple answers. Time management, and a very disciplined approach to the art and science of OSINT collection, is the key to every success.

The ever-increasing array of open sources provides a rich environment for unbridled research. OSINT managers must ensure that their staffs are aware of the degree of detail required for each OSINT product being prepared. The Internet and commercial premium online sources are seductive to the analyst. Within any OSINT effort, time spent in collection is always at the expense of analysis. The desire to continue with the

OSINT Professional Note: A recommended timetable for a standard OSINT collection and analysis task is provided below:

15 Minutes	Requirements Definition. Ensure an understanding of commander's intent.
30 Minutes	Internet Collection. Use search tools, rapidly identify top ten sites and review.
15 Minutes	Internet Table. Create Internet Table for future use and for customer's reference.
60 Minutes	Commercial Collection. Use fee sources, identify top 20 items for exploitation.
60 Minutes	Analysis. Read, understand, evaluate, and structure collected information.
60 Minutes	Production. Carefully create an analytical summary, table of contents, and slides.
4 Hours	Total time required to create any OSINT report using only internal resources.

collection and acquisition of open sources at the expense of their evaluation and presentation as an analytical product reduces the effectiveness of the OSINT contribution to the all-source effort. In few other fields is the mantra that "perfection is the enemy of good enough" more appropriate than it is for open source collection. Collection efforts can be reduced if time spent in the evaluation of the reliability and objectivity of specific open sources does not have to be replicated each time an analyst begins a project. OSINT managers should ensure that their staff maintains a dynamic compilation of the open sources that they exploit for specific issues. This reference aid will serve as the starting point for subsequent analytical tasks.

Collection Issues

There are several collection issues that always surface whenever commanders and staff first consider OSINT as a structured discipline. These include OPSEC, Copyright Compliance, Foreign Language Shortfalls, and External Networking.

Operations Security

- OPSEC is easily achievable in the OSINT environment through two measures: first, the concealment of the origin of the search through the use of trusted intermediaries; and second, the utilization of normal commercial Non-Disclosure Agreements (NDA) when necessary to protect direct discussions of a commander's concerns and intentions.

- In general, most OSINT inquiries will be amply protected by existing processes, but when appropriate, a trusted local national with information broker skills can be hired (or a Reservist utilized) to distance the inquiry from the command. It is a misconception to believe that any discussion with OSINT providers must be itself open.

- The private sector is accustomed to protecting proprietary and commercially confidential discussions. A standard private sector NDA is just as a good as a government secrecy agreement, with the added advantage that the private sector partner has a financial motivation for honoring the NDA—they want more business and discretion is part of what they are selling.

Copyright Compliance.

- In the past, many governments have felt that copyright compliance did not apply to their official needs, and some governments have resorted to the classification of open source information as a means of concealing their routine violation of private sector intellectual property rights

- It is now essential for all governments, and for all NATO elements, to learn how to properly comply with applicable copyright provisions. This is important for two reasons:

 - To maintain the highest standards of legal and ethical behavior among all NATO elements;

 - More often than not, OSINT must be shared with external private sector parties (e.g. humanitarian assistance organizations) or used as a means of exchange (pooling information on Kosovo, for example). Thus copyright compliance is a vital means of maintain future *flexibility* in the exploitation of the OSINT available.

Foreign Language Shortfalls.

- Despite the multi-cultural and multi-lingual nature of the NATO alliance, many out-of-area contingencies require

foreign language skills that are not readily available with the NATO force, or that can be identified quickly and provided with security clearances.

- Over time it is vital that each commander identifies foreign language skills as well as shortfalls and that these be consolidated and evaluated as part of the larger NATO Future Intelligence Architecture plan.

- Understanding international terrorism, insurgency, and violent internal political opposition movements, to take one example, requires competency in a number of foreign languages to include: Arabic, Catelan, Danish, Dari, Dutch, English, Farsi, Finnish, French, German, Indonesian, Irish, Italian, Japanese, Korean, Kurdish, Kurmanji, Norwegian, Pashto, Polish, Portuguese, Russian, Serbian, Spanish, Swedish, Tamil, Turkish and Urdu.

- Many of the required capabilities are within the competence of national intelligence organizations but these capabilities are unlikely to be made available to NATO commands for the exploitation of OSINT.

External Networking.

- There are four obstacles to external networking relevant to NATO competency in OSINT.

- First, there is a lack of knowledge about who the real experts are on various regional and topical issues.

- Second, there is a fear of revealing the question as an official inquiry—in some countries; there are even prohibitions against direct contacts between intelligence personnel and private sector experts.

- Third, there is the lack of funding for compensating subject-matter-experts—everything must be done on a barter or exchange of favors or information basis.

- Fourth and finally, the existing command & control, communications, computing, and intelligence (C^4I) architectures tend to prohibit routine access to the Internet, and often make it difficult if not impossible to migrate unclassified information from the Internet into classified databases.

All of these obstacles can be overcome. A major outcome of the new NATO OSINT initiative will be the definition and resolution of each of these obstacles.

Nuances of Open Source Collection

The Internet, although it will never be a completely trustworthy source for information, has become the *de facto* C^4I backbone for everyone other than the military. It is essential that our intelligence, operations and logistics staffs develop new doctrine and new methods for fully exploiting the data sources and the human experts that are easily accessible through this medium. As NATO deals with more and more non-traditional threats and more and more out-of-area as well as civil stability scenarios, OSINT will become a much more important element of the all-source intelligence solution. It is vital that every NATO commander and relevant staff member begin now to understand and plan for their OSINT needs.

Training in open source exploitation is relevant not only to the intelligence professionals, but also to all relevant staff

members who need access to open sources of information. OSINT is not the exclusive purview of the intelligence profession. The intelligence professionals should be available to reinforce the commander and their staff, but as a general rule, if a staff principal can answer his own information requirement exclusively through those open sources available to him, then that staff principal that should manage his own collection effort.

Intelligence staffs should enable all staff elements to access relevant open sources as directly as possible. Intelligence staffs should serve to facilitate the flow of OSINT and open source material while providing source evaluation and guidance. Applying this process will enable many potential RFIs to be self-satisfied and thus not submitted. A robust OSINT programme can reduce the number of unnecessary RFIs that bog-down the all-source intelligence staff with information requests that can otherwise be satisfied.

While each commander will have their preferred means of managing OSINT, what is required is that they have a formal point of contact for OSINT matters, an established process, and that they ensure that OSINT is fully integrated into every aspect of their command & staff operations.

The Internet, despite its current and projected growth, is primarily a vehicle for open collaboration, rather than a repository of knowledge. Commercial online sources such as Factiva, DIALOG, LEXIS-NEXIS, STN and Questel-Orbit have huge repositories of information that have been professional selected, evaluated, indexed, abstracted, structured, and made available in a very stable format with authoritative sourcing, formatting, and dating.

In many cases, the information provided through these services have been “peer reviewed” – an exhaustive evaluation process by established leaders in the field of study to ensure the accuracy of the information and the rigor of the research. The Internet is not a substitute for premium fee-for-service commercial online databases, and it is vital that no NATO element falls prey to this illusion.

Each commercial service, as discussed briefly in Chapter II, has its own strengths and weaknesses. A robust OSINT capability should include the understanding of and the means to exploit each service accordingly. Some are best for current news, others for legal records, and others for access to conference proceedings and dissertations.

According to some OSINT experts, only a fraction of known knowledge is available online, either through the Internet or through the commercial online databases. Grey literature, the limited edition publications that are not available through normal commercial channels, comprises a vital "middle ground" between online knowledge and human expertise capable of creating new knowledge in real time. Therefore the NATO OSINT process includes the inventory and evaluation of grey literature sources, and the development of a strategy, a budget, and a process for assuring that grey literature sources are fully integrated into the NATO future intelligence architecture.

Finally, there is the human element. As OSINT doctrine is developed, it would be helpful to think of three distinct forms of overt HUMINT support to NATO. First and foremost are internal subject-matter-experts. These are scattered across commands and within various elements of the member nations’ governments. Second are the private sector experts who have achieved a favorable reputation based on their proven record of accomplishments and publications. Thirdly, there are "local knowledge" experts, including legal travelers and local residents that are rarely exploited by resident defense attachés for lack of time or funding with which to reimburse individuals for their time and expense.

New means must be found for defining

which local knowledge and local observation is needed, and for combining direct observation by qualified NATO personnel, with out-sourced overt collection and production.

SECTION C. PROCESSING AND EXPLOITATION

Overview

After the vital role played during the collection portion of the intelligence cycle, when "knowing who knows" and being able to "mix and match" niche providers of varying pieces of the OSINT solution is essential, it is in the processing and exploitation portion of the cycle that the OSO really makes a mark.

Open sources, just like clandestine or covert sources, require the application of human judgment in order to sort out the important from the unimportant, the timely from the dated, the relevant from the irrelevant, the trusted from the untrusted. As so much of OSINT is *not* in digital form, hands-on human translation and evaluation are the most important part of processing and exploitation.

Without a dedicated set of automation tools to facilitate the processing of open source information, OSINT production will continue to be reliant upon *ad hoc* software solutions and rigorous analytical effort.

Analysis

When working from open sources, there is considerable danger for the analyst to be susceptible to unwanted biases and deception from open source authors. While it is never wise, nor an acceptable practice, to attribute as fact intelligence solely because it was received from a national intelligence agency, in those cases, the analyst is able to make certain judgments regarding how that agency managed its information prior to releasing its report. This is not always true for open sources. It is essential that the analyst remain mindful of and determine the origin of the information that has been gathered and the degree of trust that can be assigned to it. Appendix C provides a list of some common misperceptions and biases.

In the production of OSINT reports, it is crucial that the reader be aware of what is known and what is being speculated about. The analyst should always be careful to distinguish between information and fact. If the original source material is not provided

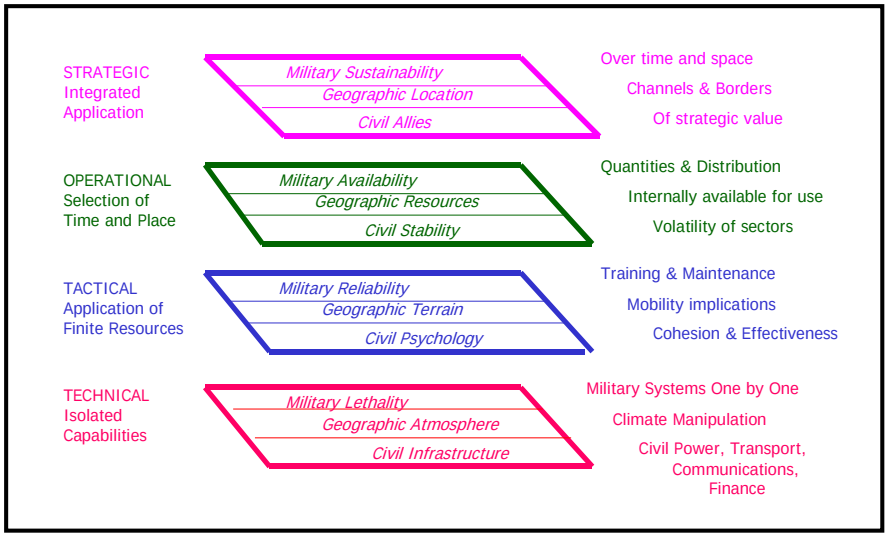


Figure 9 - Levels of Analysis Model

in full text, it is important to make reference to it and provide an assessment of the source's credibility.

If at all possible, the original sourcing information should never be separated from the open source reporting. A complete description of where the open source information was acquired, the identification of the source, the timing of both the production of the open source information and the timing of its acquisition—these all comprise fully half the value of an OSINT product. Without the sourcing pedigree, the open source substance must be considered suspect and of minimal value to the all-source intelligence analysts or the operations or policy consumers being supported.

It is also helpful when processing open source (or classified) information manually to have in mind a clear model of analysis that distinguishes between military, civil, and geographic information, and also between the levels of analysis—strategic, operational, tactical, and technical—for the threat *changes* depending on the level of analysis. This also helps the analyst to recognize gaps in their collected information, and the relationship between different types of information. One such model is provided in Figure 10 above for illustrative purposes.

Web Site Authentication and Source Analysis

Content on the Internet continues to grow at logarithmic rates. The Internet has become an essential enabling element for commerce. It is also facilitating other forms of human interaction across borders which two decades ago were unimaginable. The intelligence value of information found on the Internet is extremely variable. The dangers of creating misleading analysis through the bleeding of unevaluated biased information into the all-source intelligence picture are ever present. Therefore, the OSINT analyst must take steps with each open source to evaluate its reliability. The standard criteria for evaluation of web-sites are as follows:

Accuracy.

- Is the information that is provided consistently accurate based on other sources? The OSINT analyst is able to compare information provided from the web-site with validated all-source intelligence. Benchmarking open sources against validated all-source intelligence assists in assessing the likely accuracy of other information contained on the web-site to be used to address intelligence gaps.

Credibility & Authority.

- Does the web-site clearly identify itself? Is there merely an E-mail address or a full name, address and telephone number. *Sam Spade* (www.samspade.org) is a web service that provides various online tools to validate a web-site. These include diggers that trace routes used by the web-site. (See Web-site Analysis Guide on the following page).

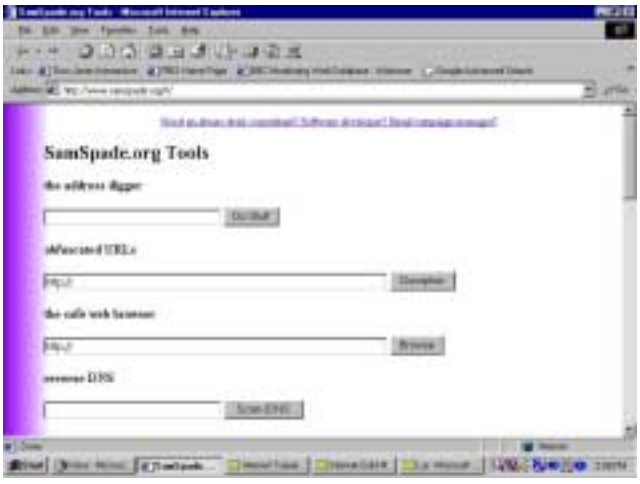


Figure 10 - Web analysis tools

- Does the web-site demonstrate a degree of influence? Do other media cite that web-site in their reporting? Has the web-site been attacked electronically or in official government statements?

- The use of free web-hosts such as Geocities.com or Cybercafe.com often suggest limited financial support for the web-site and a lack of authority in its message.

- Hit-meters/Counters that note the number of times the web-site has been visited can also provide some limited indication as to the influence of the web-site. Thought these can be misleading and should only be used as an element of an assessment of a site's authority.

Currency.

- Does the web-site provide information that is timely or are its pages dated? Some dated information can still be relevant for less dynamic topics (e.g. trade statistics) but may be misleading in tracking current events (e.g. presence of insurgent activity).

Objectivity.

- Does the web-site correspond to a known advocacy group? Does the site represent individuals or an organization? Does that site claim to speak for the organization? Is that site the main web-site or a satellite web-site that represents only a sub-element of the organization.

- To whom does the web-site link? Many sites provide a list of relevant links. These attempt to direct visitors to a community of interests that share similar interests or views. An evaluation of those links can further illuminate the views of the web-site authors.

Relevancy.

- Is the information contained on the web-site relevant to the question at hand? Many web-sites provide information related to a particular topic but do little to add to the understanding of the issue. Information provided can often be interesting but not relevant to the OSINT analyst.

WEB SITE EVALUATION CHECKLIST

Each Internet Website of potential intelligence value must be evaluated as to its suitability for intelligence exploitation *before* it is cited in OSINT reports or used as collateral information in classified reporting. The essential questions remain: who, what, where, when and why?

1. WHO? Examine the URL first. In the page scan for names, and "about" links.

What type of domain is it? (.com / .org / .edu / .gov / .mil / country code) – Is this appropriate for the material presented?
Might it be a personal page? (use of ~ in URL often suggests this)

Who wrote it? **Look for e-mail contact.**
Credentials? **Search on author's name.**
Check source code as webpage's author is often embedded in the code.

Who is the owner of the host server? **Use WHOIS and DNS LOOKUP tools at www.samspade.org to determine the registered owner of the website and evaluate this information. Does this match earlier information gathered?**

What do others say? **Search to see if others cite the author or the web-site.**
Who links to it? **In Google or AltaVista, enter the search string (*link:webaddress)* to find who links to the site. Evaluate the community of interests.**

Opinions of it? What do others think of this website?
Found in any reliable directories? **Determine if the website is contained within reliable web directories or web portals for the topic.**

2. WHAT?

Is the material presented authentic, with sources and dates?
Is data unaltered from its original source?
Note: Little value can be attached to information that is either undated or unsourced.

3. WHERE?

Where does the information originate? **Use www.samspade.org to conduct a TRACEROUTE search. TRACEROUTE will determine the path between your computer and the server hosting the information.**
Is the server located where the author purports to reside? Why or why not?

4. WHEN?

How current is the information provided? **Look for a last updated statement or dates on references.**
How often is the information maintained? Should it contain more recent information?

5. WHY?

What's the page's aim, intent?
Why was it created?
Who sponsor's the page? **Look for an "About us" entry.**

Source: Developed from material created by Joe Barker and maintained on server: www.lib.berkeley.edu.

SECTION D. SEARCHING ANONYMOUSLY ON THE WEB

Overview

While much of the OSINT cycle can be conducted openly, a robust OSINT programme should include a capability to work anonymously on the Internet. Despite the fact that all information on the web is freely available to anyone with a PC and an Internet connection, there are security dangers in searching for it.

All Internet traffic is subject to monitoring at virtually any point by elements external to your organization. It would be of little surprise that NATO was interested in insurgencies in the Balkans and Internet searches on this topic would seem natural from Alliance web addresses. Specific searches on individual leaders of insurgent groups would reveal a heightened interest and potentially reveal intentions. This sort of activity should be protected.

Being anonymous on the web may not necessarily involve deception. It is quite possible to surf the web without openly identifying your identity, purpose or intentions. This is simply a case of "I won't tell you unless you ask."

Before you even start surfing anonymously make sure you don't leave your Internet connection open to attack. You may take all the precautions necessary to hide your intentions and identity whilst surfing, but, without precautions, all the sites that you have visited and all the information you have downloaded is stored on your PC is available via your open connection, then you are vulnerable.

There is an argument for the use a firewall to stop hackers at the front door, but remember that there hasn't been a firewall yet that wasn't eventually cracked. The very expensive firewalls do a good job but it is

Elementary steps to create and maintain an anonymous WEB-Presence

Disable anything that records your activity.

If using MS Internet Explorer:

- **Turn off the cookies**
- **Clean out the history folders, and**
- **Routinely remove cached files.**

Use removable storage media to save any downloaded files to.

Only use your Internet PC for surfing. Do not use the word processor for business or personal letters.

Make sure all your connection details are anonymous.

Ensure the set up of your system is as standard as possible.

Figure 11 - Maintaining an anonymous presence

unlikely that you would want to spend so much money for a simple Internet connection. Besides if you wanted to remain anonymous on the Internet an expensive firewall is not the way to do it. It would highlight the fact that you had something to hide. The same argument applies to the cheaper firewalls. Because they are cheap they are also vulnerable. Hackers know how to get in and often see areas with firewalls as a challenge. One of the best means of security is to remain anonymous and look just like everyone else. By doing this, if a hacker chooses to attack your Internet connection whilst you are online, they would find nothing. The hacker would probably then get bored and never bother you again.

Leaving a Footprint

When you surf the Internet you cannot fail to leave a footprint. A footprint is an electronic signature that identifies you as a unique identity on the Internet during your current session. Most Internet Service Providers (ISPs) now issue a new signature to you each time you log on to surf. But whilst you are surfing during a session after log on, every site you visit retains your electronic signature. If you are trying to find information on a sensitive subject it is possible to carry out an analysis of the sites you visit and the subjects you are searching for. It would be sensible to log off and on again a number of times during a sensitive search.

Although an ISP may provide you with a new signature, part of that signature will identify the ISP. If your organization is large and has its own ISP this will identify your organization. It is always better to go through a civilian ISP whenever possible.

It is possible to use a number of different ISPs. These days there are a huge number of free ISPs available. Each country has its own list of free ISPs and details of these can be obtained via the Internet. It is possible to hide the country from which you are searching from by dialing up an ISP in another country and beginning your search from there. It is almost impossible for a hacker to identify which country your call originated from because Telecoms companies take their personal privacy obligations very seriously.

There is one thing that may identify your country of origin and that is the date and time of your search. When you surf, the date and time of your PC is stamped on the search as part of the electronic signature. If this does not match your ISP time it may indicate that you are trying to hide something, so make sure your PCs time is set to the time zone of the country of the ISP you are using.

Traffic analysis

Every web site has the capability to log the number of visitors to its site and the electronic signature of the visitor. Whilst you may be able to hide your identity, you cannot hide the fact that you have visited the site. If the number of visitors to a significant site increases dramatically then this may be an indicator that there is new or renewed interest in the subject of the site. Such a site may be set up deliberately to identify interest, for example an obscure terrorist related site.

The way to combat this is to ensure that trained personnel, in a central location do all sensitive searches. This will ensure that searches are done quickly and without repetition. The security education of all personnel who have access to the Internet is also a very important factor.

Contact with Others

There may be occasions when you may want to communicate with others to solicit information. In most cases it is beneficial to explain who you are and ask for help or information. There may be other occasions when you may not want others to know exactly who you are or whom you work for. The reasons for this must be decided on a case-by-case basis. It is reasonably easy to create an anonymous persona on the web but the following points should be noted.

It is better to employ discretion rather than deception when soliciting information on the web. This will be less publicly embarrassing later and will make an explanation of your action more reasonable.

An anonymous persona should only be used for occasional requests for information. Any development of a relationship using the Internet should be discouraged. This is the field of other specialists and without proper control can lead to embarrassment.

SECTION E. PRODUCTION

Overview

The four main elements of OSINT production are listed in Figure 12. As

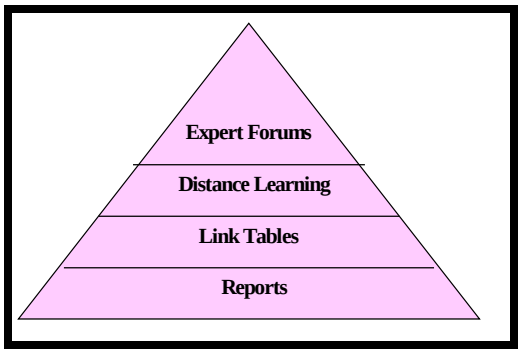


Figure 12 - OSINT Production Elements

opposed to other intelligence disciplines, OSINT relies upon outward engagement beyond the institutional confines of the intelligence staffs. Engagement is essential to the successful exploitation of open sources. This requires knowledge and understanding of information outside of intelligence channels in order to locate and exploit the best sources of information relevant to an intelligence problem and engage them in a meaningful exchange.

OSINT's four production elements will be explained within this section. While the degree of complexity will vary depending upon the intelligence requirement, those four elements will all remain applicable.

A major difference between the OSINT process and the traditional all-source intelligence process exists in how "reports" are treated. In the traditional classified intelligence process, reports are the end of the process—in the OSINT process; they are the beginning, one of four key elements in the *interactive* and *consumer-oriented* process of OSINT support.

Reports

In Chapter One, a distinction was drawn between OSIF, data that has been collated together and is of generic interest, and usually broadcast or widely disseminated and OSINT, information that has been deliberated discovered, discriminated, distilled, and disseminated to a specific consumer in order to answer a specific intelligence need.

NATO OSINT specialists will have occasion to do both kinds, but must be very clear in their own mind, when doing a report, as to whether it is an information report for general broadcast, or an intelligence report for a specific operational purpose.

A report should have an analytical summary. This is value-added expertise from a trained NATO professional who has first screened and integrated multiple elements into an underlying framework, and then devised an executive summary that can stand on its own.

Generally a Report, e.g. a report on Kosovo, will have more than one section, for instance, sections on political, military, insurgents, health, police, and external assistance. Each section should in turn have a short summary, no more than a paragraph in length. The section summaries can be used to create the overall report summary, but should be further distilled and not simply strung together.

Within each section (or linked to each section summary if done in a web-based format) should be between one and five key items of raw information—whether a transcript from a news conference, or a wire service release, or a commercial image, or an extract from a foreign military map.

A major difference between OSINT and other clandestine or covert sources is that OSINT strives to provide concurrently both analytical value and direct access to raw materials. OSINT sources rarely require protection. Text-based products can be stored and disseminated easily by electronic means.

By providing the consumer (the commander, the operator, the logistician, or the all-source intelligence analyst) with direct convenient access to the best of the raw materials, the OSINT analyst is enabling the consumer to dig deeper if they chose to while satisfying the initial RFI.

Reports should always show, on the first page, the date and hour at which collection (not production) was cut off, and the time period in days and/or hours that the report covers. Reports can be organized by source (Internet, Commercial Online, Grey Literature, and Experts) or by topic. They should always identify the author and if appropriate the reviewer of the Report, and provide complete contact information so that readers may quickly ask follow-up questions of the originator.

COUNTRY (e.g. Sri Lanka)

TOPIC (e.g. Economy)

DATE OF INFORMATION (e.g. 26 March 2001, 1500EST)

ANALYTICAL SUMMARY (new value-added analytic summary)

RAW INFORMATION 1 (best of 20 read sources from 200 screened sources)
RAW INFORMATION 2 (best of 20 read sources from 200 screened sources)
RAW INFORMATION 3 (best of 20 read sources from 200 screened sources)
RAW INFORMATION 4 (best of 20 read sources from 200 screened sources)
RAW INFORMATION 5 (best of 20 read sources from 200 screened sources)

Figure 13 - Representative report structure

Link Tables

Internet search engines, even recommended meta-search engines, have severe limitations. By some accounts, any one search engine will cover only 10-15% of the visible web, and even all the search engines working together will overlook what is known as the "deep web." The deep web consists of complex sites with many levels, many free and some by subscription, where search engines are simply ineffective. While some tools such as the affordable software programme *Lexibot* are available to assist in collection from the "deep web", considerable time is spent in the identification and analysis of open sources relevant to the information requirement. For this reason, a major aspect of the OSINT support process is the skilled creation of Internet Link Tables that serve as a ready reference for the commander or staff officer who desires to rapidly scan external information sources without necessarily requesting a report. This browsing endeavor can often help the commander or staff principal reflect on their requirements and better articulate their next demands for finished OSINT. An Internet Link Table should generally be in the form of a Table, such as is illustrated In Table 5 above. By using the Word Table feature, this allows the sorting of the information based on either the Rank or Weight assigned to the site, the URL or title of the site, or the description category of the site. Over time, as various NATO components cooperate and share Link Tables with other allies forces such as the various regional Joint Intelligence Centers, a very comprehensive directory of web resources, one that is tailored to NATO's needs, should emerge.

Ranking	Link	Source
10	http://allafrica.com/libya/	**All Africa News – Libya –** Up-to-date news on Libya, in English and in French.
10	http://memory.loc.gov/frd/cs/lytoc.html	**Library of Congress Libya Country Study** – Excellent, in-depth country study
10	http://members.aol.com/LibyaPage/	**Libya Resources on the Internet –** Excellent, comprehensive site, includes news, Qadhafi info, maps and satellite photos, military and intel, etc.
10	http://www.un.int/libya/	**The Permanent Mission of Libya to the UN** Website **–** Includes press releases & statements, ambassador's remarks and links.
10	http://www.nfsl-libya.com/	**The National Front for the Salvation of Libya** - The NFSL is an opposition movement against the dictatorial regime of Qadhafi in Libya, and was formed in October 1981.
8	http://www.libyamazigh.org/	**Libyan Amazigh** site. Contains info on Libya's Amazigh (Berber) culture, language and history.
8	http://www.libyaonline.com/index.html	**Libya Online** Website – Contains basic facts about Libya, tourism, business, arts, literature and sports.

Table 5 - Example of Internet Link Table

Distance Learning

The Internet, while rendering a major service to those who would like to share information efficiently and also interact inexpensively with diverse people all over the world, has also reduced the productivity of even experienced personnel. Constant interruptions and distractions through diversions to less important information are

core factors. For this reason, there is an urgent need for Distance Learning modules on all countries and topics that are of interest to NATO. The objective is to ensure that all new personnel, and especially new action officers, have an online resource that can serve as a sophisticated turnover file and reference point. This is also a place where unclassified biographic information can be made available, and where annual reviews of each country or topic can be placed.

The U.S. Pacific command initiative known as the Virtual Information Center is an good example of this process. It can be accessed at www.vic-info.org.



Figure 14 - Homepage of US PACOM OSINT Centre

Expert Forums

A number of software programs exist with which to manage a variety of Expert Forums, including private teams with their own newsletters, calendars, and automated email alerts whenever new information is posted. One of the most popular is the Alta Vista Forum. One of the newest, with powerful security features, is offered by Groove Inc. (www.groove.net) and represents the emerging shift in communications and computing power away from centralized server farms toward what is known as "peer to peer" edge units.

Expert Forums can be internal, external, or some combination of the two. Once experts have been identified, they may be invited to join the Expert Forum sponsored by any NATO element. This should be done with the understanding that they will contribute their time and insights on an occasional basis, in return for being granted access to the OSINT being produced by the NATO element sponsoring the Expert Forum. Such a forum can also be a place where individual experts "audition" for short-term consulting contracts and where the biographies of available efforts can be made available for anonymous review by potential NATO employers.

Expert Forums should consist of several parts, all of them of potentially great value to the NATO OSINT process. First, while it is possible to register anonymously for a forum, the greatest value comes from an open registration that includes a photo, biographic note, and complete contact information. Second, the forum will quickly self-organize, with a variety of topics to which an individual can not only contribute observations, but to which they can upload documents, images, even video. The flexibility and scalability of these forums cannot be overstated—but they do have one major flaw: at this time, it is not possible to apply visualization or other technologies to the varied contents of a forum—each item must be copied down to a master database first.

Soon the technology will be available to index and abstract all information contributed to a forum, at which time the best of all worlds will be available: distributed experts able to cast a wide net, and a centralized "banking" function for information freely contributed by various parties. Third, the forum permits the rapid organization of private working groups, and offers calendar, newsletter, and other

coordination features. Fourth and last, the forums can provide an automatic email alert to any member whenever new information is posted to a topic of interest to them, relieving them of the need to constantly check the forum site.

SECTION F. DISSEMINATION AND EVALUATION

Overview

The major difference between OSINT and the other intelligence disciplines is that the latter are inherently classified: OSINT can be shared with *anybody* that the commander deems appropriate, without having to request security or political clearances.

This makes it extraordinarily valuable in non-article V operations as well as in dealing with civil sector coalition partners—including NGO that traditionally distrust the military in general and intelligence professionals in particular. OSINT has become even more valuable in the 21st Century, as there has been a major change in the over-all C^4I paradigm.

As NATO continues to evolve and transform itself in response to the many new challenges, the importance of OSINT will continue to evolve. These new challenges include non-traditional non-military challenges requiring coordinated action with non-governmental and humanitarian relief organizations.

OSINT appears to offer a very substantial advantage as a prime intelligence source and method with which to achieve consensus and a common understanding of the shared area of operations.

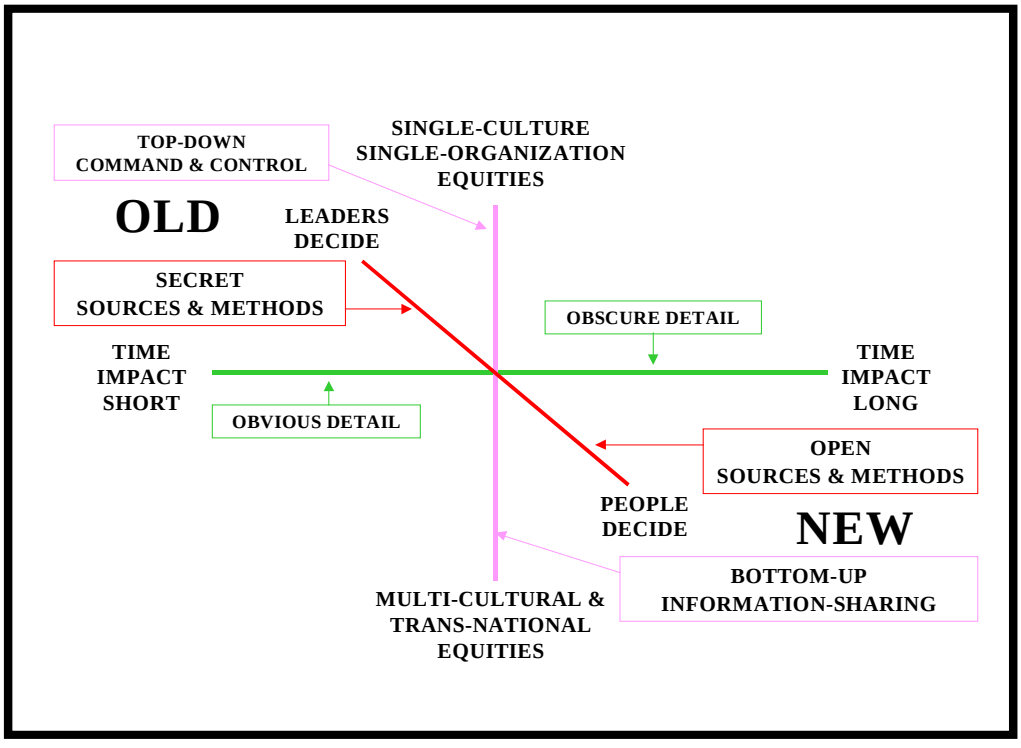


Figure 15 - Emerging Paradigm for Information Sharing

Dissemination Methods

Once open source information has been developed into OSINT, it can be disseminated via the NATO WAN in a "push" mode, or it can be "pulled" off on demand.

The limitations placed on its dissemination are based on the security policies of the organization producing it. While some OSINT products may be shared openly, others may provide details of interests or intentions and should therefore be restricted in their dissemination. The dissemination policy should be driven by the mission requirements. The approach should nonetheless be flexible to fully leverage the ability that the production of OSINT products provides for the engagement of non-NATO elements in security discussions or the development and dissemination of a common view of the operating area.

Within the NATO Intelligence Architecture, options exist for the dissemination of OSINT products via the classified NATO WAN or directly through the Internet. The advantages of the NATO WAN are the direct access afforded to the operations and policy staffs at all levels, including deployed units, as well as the security afforded by the use of a classified system. The principal disadvantage of the NATO WAN for OSINT dissemination is the necessary separation of the products from their source material. Without a direct linkage between an OSINT product and the sources of information, the recipient is less able to drill deeper for additional information, reach the original author, or further evaluate the original sources of the information.

Another option is the use of a Virtual Private Network (VPN). A VPN is a restricted community of interest that communicates on the Internet but use security safeguards to limit the access from others who are not members. By using a VPN, OSINT products can be accessed safely and with working links directly to the original source material. Link tables can also be maintained that enables the rapid collection of information. Other OSINT centres within NATO member countries have direct access to the Internet; few have access to the NATO WAN. A VPN provides the means with which to exchange OSINT products with other OSINT centres across NATO. Finally, the use of a VPN provides the means with which to disseminate OSINT products with non-NATO elements such as NGOs and other international organizations as mission requirements demand.

For these reasons, exploring the feasibility and desirability of a VPN to support the NATO OSINT Initiative remains a priority. SACLANT has begun a trial VPN with the U.S. Open Source Information System (OSIS) to examine the viability of linking NATO OSINT production centres with U.S. OSINT holdings.

Virtual Intelligence Community

The NATO OSINT initiative is the first major multi-national OSINT initiative ever undertaken. While there is much still to learn from those member nations that adopted OSINT as an independent discipline in the 1990's, as well as from the emerging business intelligence community (such as represented by the Society of Competitive Intelligence Professionals at www.scip.org), it is NATO that is leading in the establishment of formal doctrine and tables of organization and equipment specifically earmarked for OSINT. It is helpful, in contemplating this activity, to understand that there is a substantial but still fragmented community of interests with whom NATO could co-develop many OSINT initiatives. This community is illustrated in Figure 16.

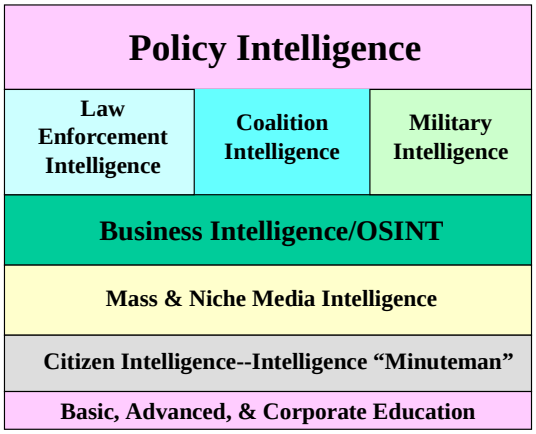


Figure 16 - Elements of a virtual intelligence community

As commanders and their staff evaluate their needs for OSINT, and new methods as well as budget deficiencies, SCs and subordinate commands should seek to establish a constant process of interactive liaison with each of the elements of the "virtual intelligence community" shown here. In this fashion, NATO intelligence could benefit from a greater OSINT effort that cuts across bureaucratic and cultural boundaries, and leads to improved cost efficiencies and new forms of information sharing.

CHAPTER IV
OSINT AND THE EMERGING FUTURE INTELLIGENCE ARCHITECTURE OF NATO

SECTION A. BLENDING OSINT INTO THE ALL-SOURCE PROCESS

Overview

Apart from the importance of OSINT as a means of establishing consensus and a common view with external parties about the shared area of operations, OSINT is absolutely vital to the all-source intelligence process. OSINT provides the historical background information, the current political, economic, social, demographic, technical, natural, and geographic context for operations, critical personality information, and access to a wide variety of tactically useful information about infrastructure, terrain, and indigenous matters. The relationship between OSINT, the traditional collection disciplines, and all-source analysis is shown in Figure 17.

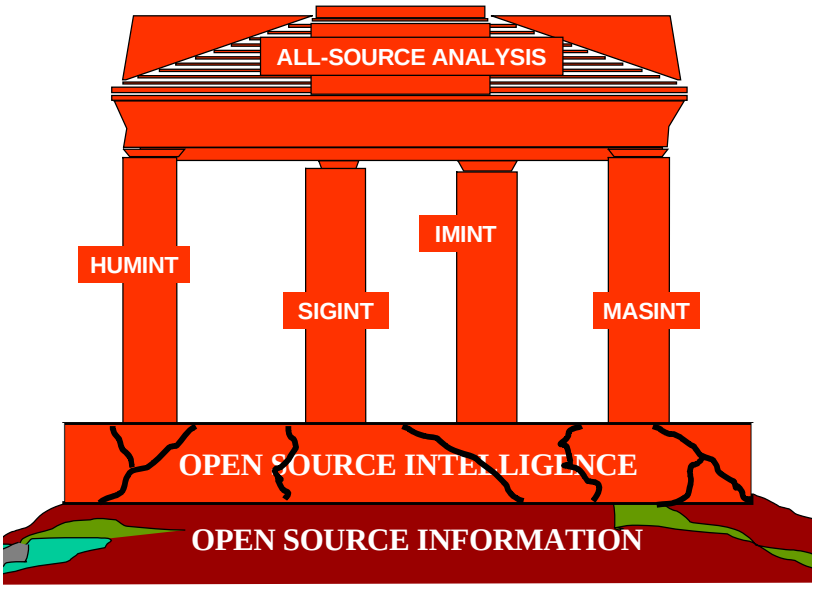


Figure 17 - Open Source - All-Source relationship

Cracks are shown in the OSINT foundation to emphasize that this vital element of the all-source intelligence process has been too long neglected. Following the publication of the Alliance's Strategic Concept in April 1999, OSINT is even more important. NATO, along with other international organizations, is now striving to understand ethnic conflict, water and food scarcity, mass migrations, the collapse of public health across entire continents, transnational crime, and all of the small wars—and the potential threat of large wars—that remain a traditional responsibility. OSINT can and should be integrated into every aspect of the all-source process, from collection through production.

Nations and NATO commands differ fundamentally in their approaches towards OSINT. Both begin with intelligence needs that lead to the generation of intelligence requirements. The approaches diverge at that point. While nations may use OSINT to guide classified collection, NATO rarely has classified collection means beyond the tactical level and those assets are largely restricted to theatres in which forces are already deployed.

NATO commands can use OSINT-V to satisfy intelligence gaps for a large number of its intelligence needs. While nations are able to turn to classified intelligence collection, NATO can and should use the OSINT process described as the first step in its collection process. Too often, NATO commands have defaulted to sending RFIs to nations rather than seeking first to address their intelligence requirements themselves. The range of open sources now within reach of NATO intelligence staffs provides other options.

The new Strategic Concept articulated a vision for the Alliance that is largely focused on non-traditional operating areas and transnational threats. The intelligence services of the NATO member countries are also struggling to deal with a similar problem set. These areas and interests, while not well covered by traditional intelligence production are well addressed in open sources. Rather than relying solely upon nations for intelligence products, NATO intelligence staffs should develop their own network of open sources as the starting point for the compilation of their intelligence assessments.

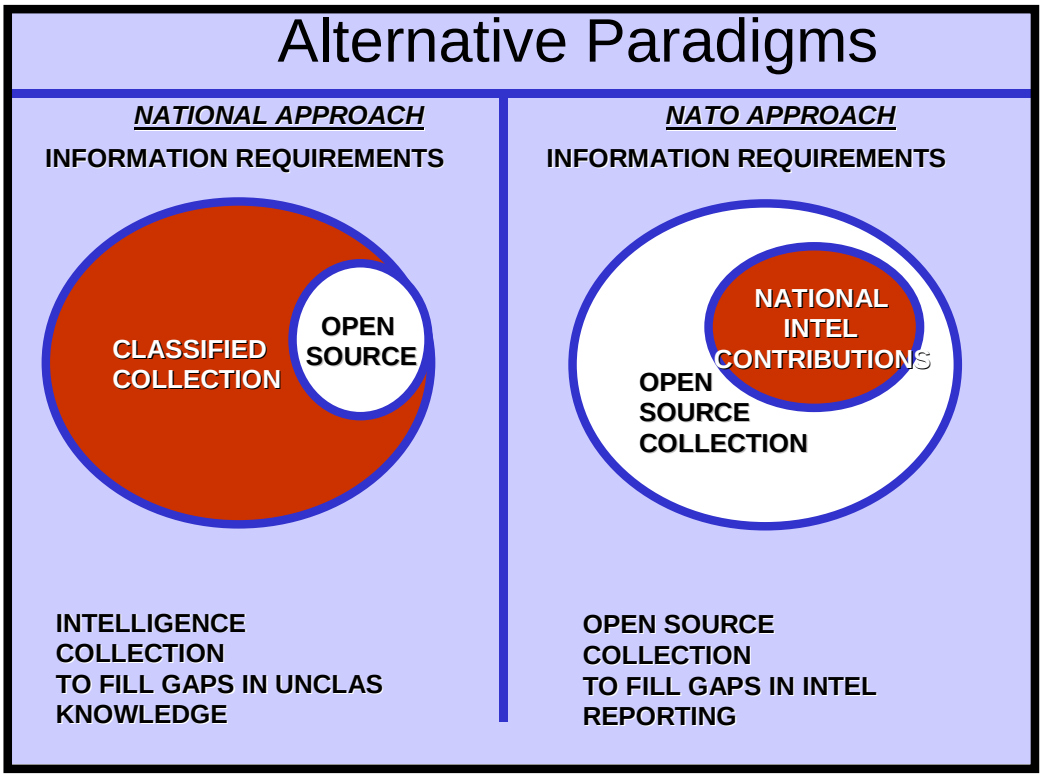


Figure 18 - Alternative Paradigms between NATO and National OSINT Approaches

Direction

Open information sources are as easy for NATO leadership to access as they are for their intelligence staffs. No longer are intelligence staffs in a position to regulate the flow of relevant information to the commander or his staff. Virtually all decision-makers make regular use of open sources to varying degrees. Knowledge of those sources routinely consulted by the staff principals is an important means with which to stay ahead of their intelligence needs.

Rather than attempting to stem the use of open sources by the commander or his staff, an effective OSINT effort facilitates it. Intelligence staffs at both Strategic Commands (SCs) have access to specialized information retrieval tools and commercial sources. In addition, both SCs are in a position to provide training and advice on the effective retrieval of information from open sources. An OSINT process should include the provision of validated information sources for each issue that affects the command. The provision of Link Tables as well as quality assessments of other information sources is an essential OSINT product.

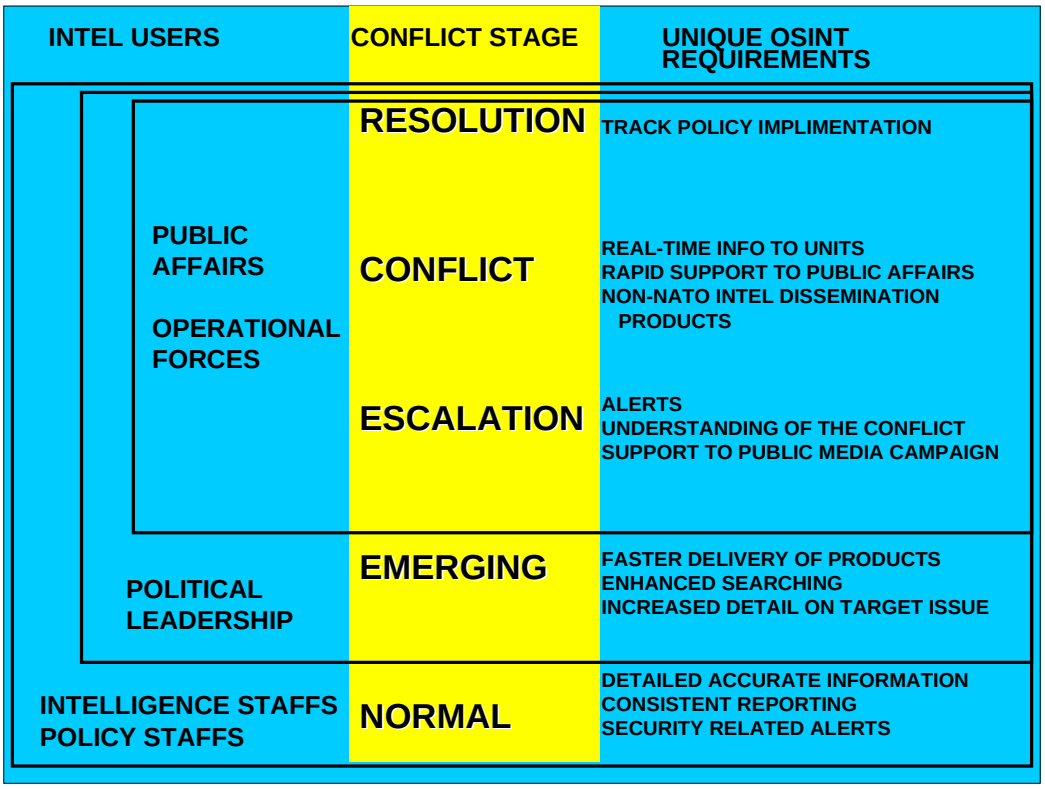


Figure 19 – Unique OSINT Requirements across the Conflict Spectrum

Typically, informed decision-makers make reasoned requests for intelligence. While not always the case, this statement generally holds true. With an appreciation for what is widely known, intelligence users will tend to restrict their requests to that information which they do not already have available to them.

OSINT can support the direction phase of an

all-source intelligence effort through discovery of an issue or providing context with which to understand issues.

The intelligence problem varies depending on the nature of the issue being addressed, which elements of the staff are engaged and what degree of information is required. Figure 19 shows a representative range of information products that a robust OSINT capability can provide.

Assuming an OSINT capability is in place in advance of a crisis, it is likely that the leadership will have had access to quality open source products prior to the onset of mission requirements. In that case informed RFIs can be expected. If there is no familiarity with the issue, decision-makers can be directed to either established OSINT products or open sources of information that can be made available through access to an information portal such as a VPN of another network. Finally, an OSINT collection effort can be initiated to quickly produce relevant background information. This immediate OSINT effort will quickly establish what is easily known about the subject and guide the priorities for classified collection and all-source production.

Collection

Within the intelligence cycle, the collection phase includes the translation of the intelligence need into a collection requirement, the definition of a collection strategy, the selection of the collection sources and the actual information collection. Open sources should be the first recourse in the collection process. OSINT saves money in reducing unnecessary classified collection. In a NATO context, it saves time as RFIs to nations require sufficient lead-time for them to be properly addressed.

While open source information is not free, the costs pale in comparison to those of the classified collection disciplines. If open sources can be collected to produce an OSINT product that addresses completely or to a large degree the intelligence need, classified collection resources can be more effectively deployed elsewhere.

While nations have classified collection capabilities, these are expensive and must always be used wisely. NATO has no tasking authority over national intelligence collection capabilities. Its reliance upon intelligence contributions from nations makes it incumbent upon its intelligence staffs to know what can be known without technical collection.

Open sources have always been used by intelligence organizations. Open sources have typically been referred to as *collateral reporting*. In fact, all single source intelligence disciplines refer to information provided by another intelligence discipline as *collateral reporting*.

However, when this collateral reporting is maintained with a systematic disciplined approach as discussed in this OSINT Manual, the “collateral” grows in its own utility. Instead of being acquired once and used by one intelligence element, it is acquired once and applied across a broader range of the intelligence process from streamlining collection to increasing dissemination.

OSINT’s four main contributions to classified collection are: tip-off for classified sources; targeting of those sources; context and validation to better understand material collected from classified sources, and; providing plausible cover to protect the classified source.

Tip-off.

- Open sources are particularly well suited to providing *tippers* for other collection disciplines. The reduction in the number of denied areas since the end of the Cold War and the advent of cheap international transportation options have enabled greater media access than ever before. Internet NEWSGROUPS, wire services and other traditional print and broadcast media are all within the reach of anyone.

- The Internet remains a primary means with which to gain access to these sources. While traditional print and broadcast media are restricted in the amount of information that they can provide, the Internet has provided virtually limitless dissemination capabilities for information producers. Rather than the editor's selection of stories, the Internet provides the means with which to gain access to all stories filed with all of the wire services depending on the degree of access that is purchased.

- A number of services provide news alerts that are either free of charge or low cost. Non-traditional sources of information include those who witness important events and who post messages on the Internet about what they have seen. While prone to disinformation, this is another source of information that must be evaluated like all others. Those who witness an event and publish on-line or forward emails to their communities of interest can provide the first indication of an event even before media publication.

Targeting.

- While OSINT will often be able to address elements of an intelligence problem quickly and efficiently, OSINT will never invalidate the need for classified collection capabilities.

- When intelligence gaps can be addressed without the need to task classified collection sources overall demand upon limited collection resources decreases. This permits concentration of effort on those issues that can only be discovered through classified collection.

- This model of complementary collection permits both open and classified sources to be optimized for a particular intelligence problem, while at the same time, affording the all-source analyst the ability to use the classified collection products to validate the OSINT products.

Context/Validation.

- Supplemental open source reporting can provide the means with which to place classified reporting into context. Classified reporting, particularly current intelligence reporting, often fails to provide the necessary background information with which to tailor the information to the needs of the recipient or to explain the nuances of the situation.

- While imagery can provide knowledge of ships alongside piers, additional information from open sources can provide an understanding of the cargo that the port handles or the schedule of the ship. Similarly, UN reporting on agriculture production shortfalls in a particular country will give insight into population movements detected with national technical means.

Plausible Cover.

- OSINT is particularly useful in protecting classified sources and methods. The discovery of an open source that corroborates classified



Figure 20 - Commercial imagery of San Diego naval base

reporting may increase the releasability of the initial information by providing a plausible alternate source. This also has applicability to the staffing of requests for the sanitation of classified reporting.

- A thorough understanding of information that is available in unclassified channels facilitates the discovery of plausible alternate sources to classified intelligence reporting. This ultimately increases the ability of intelligence staffs to release intelligence information to non-NATO elements within missions.

Processing

The objective of intelligence processing is the creation of an intelligence product that is value-added, actionable information tailored to a specific user. All-source analysis with its fusion of all relevant and validated sources of information remains the best means to convey intelligence to the user. This process includes both classified and OSINT reporting as appropriate. In most cases, NATO will serve as one element of an international crisis response. Experience has shown that these operations likely include the leading of a broader coalition alongside non-NATO troop contributing nations (NNTCNS). The processing of intelligence products to support the information needs of both the NATO-led force and the international response elements is greatly enhanced with a robust OSINT capability.

Intelligence products can be prepared with a tear-line – classified intelligence restricted in its dissemination above the line and sanitized information that can be more broadly disseminated below the line.

OSINT–V products can be produced specifically tailored for the broader coalition audience but validated by the all-source process. During actual operations, the need to disseminate to non-NATO elements includes not only their operational forces, but also their political liaison elements at NATO headquarters in Brussels.



Figure 21 - Nature of international operations

The maintenance of information sources that can be disseminated outside of NATO channels can often prove essential to both establishing a common view of the operating area and initiating an exchange with other entities that can contribute to the understanding of an issue.

Dissemination

As stated earlier, OSINT is itself optimized for dissemination through VPNs. This enables ready access to the original source material, direct interaction with other related open sources and access to other OSINT producers.

The dissemination of OSINT products as stand-alone intelligence products on classified systems should also be encouraged. OSINT as either stand alone products or as collateral reporting adds to the body of knowledge on a particular issue. Intelligence staffs at all levels should be able to benefit from the effort put into their production. It is rare that all subordinate commands will have access to every intelligence system. Thus, efforts should be made to ensure that products are available on all intelligence dissemination systems as security constraints permit.

Typically, the lower the classification of an intelligence product the wider is its uses. If decision-makers are able to leave their offices with an intelligence product, it is more likely that it will receive undisturbed attention. OSINT products provide the means to place high quality low-classification or unclassified products in the hands of intelligence users. This is only possible if they are disseminated on systems typically used to deliver other forms of intelligence.

The objectives of a robust OSINT capability should be to increase the range of information available to intelligence users and to facilitate interaction with non-NATO elements as appropriate. The dissemination options developed should seek to achieve these two objectives.

APPENDIX A: GENERAL REFERENCE LINK TABLE

Maps:

World Ports	http://www.world-ports.com/
United Nations	http://www.un.org/peace/kosovo/pages/kosovo1.shtml
CIA World Factbook	http://www.odci.gov/cia/publications/factbook/indexgeo.html
Quick Maps	http://www.theodora.com/maps/abc_world_maps.html
CNN Video Select	http://europe.cnn.com/video/netshow/
The Place For Maps	http://www.maps.com/?AID=41160&PID=186662
Map Quest	http://www.mapquest.com/
Expidia.com	http://www.expedia.com/pub/Agent
Media Maps.com	http://media.maps.com

News:

NBC Daily	http://www.nbc.com/
Bloomberg	http://www.bloomberg.com
MSNBC	http://www.msnbc.com
CNN Videoselect	http://europe.cnn.com
Fox News	http://www.foxnews.com
BBC Monitoring	http://news.monitor.bbc.co.uk/
BBC NEWS	http://news.bbc.co.uk/
CBS NEWS	http://www.cbs.com/daytime/bb/show_update/update.shtml
CNBC Dow Jones Business Video	http://cnbcdowjones.com/msnbc
CNET Today	http://news.cnet.com
ABC News	http://abc.go.com
CNN	http://www.cnn.com
The Sunday Times	http://www.information-britain,co.uk/news.sundaytimes.htm"
News Now 1401	http://www.newsnow.co.uk/
MSN News	http://www.msn.com
Real Radio	http://realguide.real.com/tuner/?
ABCNews	http://abcnews.go.com/
Business Journal	http://business.netscape.com/business/main.tmpl
Fox News	http://www.foxnews.com/
International News	http://www.internationalnews.com/
AJR News Link	http://ajr.newslink.org/
ITN News British	http://www.itn.co.uk/
The World News	http://www.theworld.org/
Out There News	http://www.megastories.com/index.shtml
CNN International	http://europe.cnn.com/CNNI/
The Times	http://www.thetimes.co.uk/
LA Times	http://www.latimes.com/
Jerusalem Post	http://www.jpost.com/
Belfast News	http://www.belfasttelegraph.co.uk/index.shtml
The Washington Post	http://www.washingtonpost.com/
South China Morning Post	http://www.scmp.com/
The Japan Times	http://www.japantimes.co.jp/
Yahoo	http://www.yahoo.com
The CNET Channel	http://channel.cnet.com/Channel/Intro/index.htm
The Wall Street	http://interactive.wsj.com/ie4intro/index.htm

Conflict:

United Nations High Commission For Refugees	http://www.unhcr.org
Weapons Of Mass Destruction	http://www.fas.org/irp/threat/wmd_state.htm
Terrorism Research	http://www.terrorism.com/index.shtml

Counter Terrorism	**http://www.state.gov/www/global/terrorism/**
Intelligence Net	**http://www.intellnet.com**
Federation of American Scientist	**http://www.fas.org**
War Information	**http://www.psycom.net/iwar.1.html**
China's Military Developments	**http://www.commw.org**
Kosovo Info	**http://perso.respublica.fr/infokosovo/**
Institute for Global Communications	**http://www.igc.org**
Anti War Home Page	**http://www.nonviolence.org/archivedsites/iraq/**
Missle, Threats & Response	**http://www.cdiss.org/tempor1.htm**
Modern Day Piracy	**http://www.geocities.com/Tokyo/Garden/5213/modern.htm**
KORB Marine Links	**http://www.pg.gda.pl/~korab/kor_lnk.html**
Piracy Centre	**http://www.iccwbo.org/ccs/menu_imb_piracy.asp**
The Panama Canal	**http://www.pancanal.com/eng/index.html**
Royal Australian Navy Sites	**http://www.navy.gov.au/html/links.htm**
Royal Navy Association	**http://www.royal-naval-association.co.uk/page6.htm**

Regional Information:

CIA World Factbook	**http://www.odci.gov/cia/publications/factbook/indexgeo.html**
Geo Spatial Information	**http://www.geoplace.com/**
Geographic Learning Site	**http://geography.state.gov/htmls/plugin.html**
Association For Geographical Information	**http://www.agi.org.uk/**
Salam Iran	**http://www.salamiran.org/IranInfo/General/Geography/**
Limes Geo review	**http://www.limesonline.com/doc.navigation**

Reference:

Britannica	**http://britannica.com/**
Dictionary	**http://Dictionary.com**
Every Rule	**http://Everyrule.com**
FBIS	**http://199.221.15.211/**
Central Intelligence Agency	**http://www.cia.gov/**
Indian Naval Review	**http://www.janes.com/defence/naval_forces/gallery**
Bureau for International Narcotics and Law Enforcement Affairs	**http://www.state.gov/www/global/narcotics_law/**
Archive Site for State Department information	**http://www.state.gov/index.html**
Naval Technology	**http://www.naval-technology.com/index.html**
Janes Naval Forces	**http://www.janes.com/defence/naval_forces/index.shtml**
Encyclopedia	**http://Libraryspot.com**
World Fact Book	**http://Worldfactbook.com**
The Intelligence Community	**http://www.odci.gov/ic/**
One World	**http://www.oneworld.net/**
Yahoo	**http://www.yahoo.com**
Lloyds List	**http://www.lloydslist.com**
Ask Oxford	**http://www.askoxford.com/**
(WMD) Weapons Of Mass Destruction	**http://www.fas.org/irp/threat/wmd_state.htm**
Incident Response	**http://www.llnl.gov/nai/rdiv/rdiv.html**
Conference For Middle East Peace	**http://www.cmep.com/**

APPENDIX B: TRAINING LINK TABLE

Below are a few of the essential references that are available online. Please note that the NATO guide *Intelligence Exploitation of the Internet* is also available online at the SACLANT Intelligence homepage on the NATO WAN. This publication is regularly updated with the best resources available to guide in the use search strategies and tools to exploit open sources available on the Internet. The Open Source Intelligence Proceedings include over 5,000 pages from over 500 international authorities including the (then) Director General of the International Red Cross and many other European and Asian experts, and comprise the "information commons" on the state of the art for open source intelligence.

OSINT Presentation to SHAPE/PfP Flags	http://www.oss.net/Papers/white/SHAPE.ppt
Information & Intelligence Bibliography	http://www.oss.net/Papers/white/23-BibliographyAnnotated.rtf
Eight Self-Paced OSINT Lesson Plans	http://www.oss.net/DispFrame.html?Papers/training/index.html
Creating an OSINT Cell (DIA Report)	http://www.oss.net/DispFrame.html?Papers/white/DIAReport.html
Business Intelligence Primer (1994)	http://www.oss.net/DispFrame.html?Papers/white/THETHEORYANDPRACTICEOFCOMPETITORINTELLIGENCE.html
Open Source Intelligence Proceedings	http://www.oss.net/Proceed.html
Index to OSINT Proceedings	http://www.oss.net/Papers/white/index.rtf
OSINT and the Military	http://www.oss.net/Proceedings/95Vol1/aab0aw.html
Canadian Intelligence Studies	http://www.sfu.ca/igs/CASIS/
Come Back Alive "Ground Truth"	www.comebackalive.com/df/index.htm
Future of Intelligence	www.future-intel.it
History of Intelligence	http://intelligence-history.wiso.uni-erlangen.de
Intelligence Resource Program	http://www.fas.org/irp/index.html
Links to International Media	http://www.esperanto.se/kiosk/index.html
Literature of Intelligence	http://intellit.muskingum.edu
Open Directory Project	http://dmoz.org/
Strategic Intelligence	http://www.loyola.edu/dept/politics/intel.html
Form for Evaluating the Value of Web Pages	http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/EvalForm.pdf
Internet Training Course by Russ Haynal	http://navigators.com/fbis.html
Berkeley University Tutorial for Finding Information on the Internet	http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/FindInfo.html
Search Techniques for the Invisible Web	http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/InvisibleWeb.html#Table
Techniques for “Searching Upstream”	http://websearch.about.com/library/weekly/aa061101a.htm?once=true&

APPENDIX C: CATEGORIES OF MISPERCEPTION AND BIAS

Evoked-Set Reasoning: That information and concern, which dominates one's thinking based on prior experience. One tends to uncritically relate new information to past or current dominant concerns.

Prematurely Formed Views: These spring from a desire for simplicity and stability, and lead to premature closure in the consideration of a problem.

Presumption that Support for One Hypothesis Disconfirms Others: Evidence that is consistent with one's preexisting beliefs is allowed to disconfirm other views. Rapid closure in the consideration of an issue is a problem.

Inappropriate Analogies: Perception that an event is analogous to past events based on inadequate consideration of concepts or facts or irrelevant criteria. Bias of "Representativeness".

Superficial Lessons From History: Uncritical analysis of concepts or event, superficial causality, over-generalization of obvious factors, inappropriate extrapolation from past success or failure.

Presumption of Unitary Action by Organizations: Perception that behavior of others is more planned, centralized, and coordinated than it really is. Dismisses accident and chaos. Ignores misperceptions of others. Fundamental attribution error possibly caused by cultural bias.

Organizational parochialism: Selective focus or rigid adherence to prior judgments based on organizational norms or loyalties. Can result from functional specialization. Groupthink or stereotypical thinking.

Excessive Secrecy (Compartmentation): Over-narrow reliance on selected evidence. Based on concern for operational security. Narrows consideration of alternative views. Can result from or caused organizational parochialism.

Lack of Empathy: Undeveloped capacity to understand others' perception of their world, their conception of their role in that world, and their definition of their interests. Difference in cognitive contexts.

Mirror-Imaging: Perceiving others as one perceives oneself. Basis is ethnocentrism. Facilitated by closed systems and parochialism.

Ignorance: Lack of knowledge. Can result from prior-limited priorities or lack of curiosity, perhaps based on ethnocentrism, parochialism, and denial of reality, rational-actor hypothesis (see next entry).

Rational-Actor Hypothesis: Assumption that others will act in a "rational" manner based on one's own rational reference. Results from ethnocentrism, mirror imaging, or ignorance.

Denial of Rationality: Attribution of irrationality to others who are perceived to act outside the bounds of one's own standards of behavior or decision making. Opposite of rational-actor hypothesis. Can result from ignorance, mirror imaging, parochialism, or ethnocentrism.

Proportionality Bias: Expectation that the adversary will expend efforts proportionate to the ends he seeks. Interference about the intentions of others from costs and consequences of actions they initiate.

Willful Disregard of New Evidence: Rejection of information that conflicts with already-held beliefs. Results from prior commitments, and/or excessive pursuit of consistency.

Image and Self-Image: Perception of what has been, is, will be, or should be (image as subset of belief system). Both inward-directed (self-image) and outward-directed (image). Both often influenced by self-absorption and ethnocentrism.

Defensive Avoidance: Refusal to perceive and understand extremely threatening stimuli. Need to avoid painful choices. Leads to wishful thinking.

Overconfidence in Subjective Estimates: Optimistic bias in assessment. Can result from premature or rapid closure of consideration, or ignorance.

Wishful Thinking (Pollyanna Complex): Hyper-credulity. Excessive optimism born of smugness and overconfidence.

Best-Case Analysis: Optimistic assessment based on cognitive predisposition and general beliefs of how others are likely to behave, or in support of personal or organizational interests or policy preferences.

Conservatism in Probability Estimation: In a desire to avoid risk, tendency to avoid estimating extremely high or extremely low probabilities. Routine thinking. Inclination to judge new phenomena in light of past experience, to miss essentially novel situational elements, or failure to reexamine established tenets. Tendency to seek confirmation of prior held beliefs.

Worst-Case Analysis (Cassandra Complex): Excessive skepticism. Reflects pessimism and extreme caution, based on predilection (cognitive predisposition), adverse past experience, or on support of personal or organizational interest or policy preferences.

Source: Lisa Krizan. *Intelligence Essential for Everyone*. Washington D.C. Joint Military Intelligence College, June 1999.

APPENDIX D. LIST OF ABBREVIATIONS

AIIB – Association of Independent Information Brokers
AOO - Area of Operations
API - Application Program Interfaces
BBC - British Broadcasting Corporation
COSPO - Community Open Source Program Office
EEI - Essential Elements of Information
FBIS - Foreign Broadcast Information Service
ICRC - The International Committee of the Red Cross
ISPs - Internet Service Providers
MCCIS – Maritime Command and Control Information System
NATO - North Atlantic Treaty Organization
NDA - Non-Disclosure Agreements
NGO - Non-Governmental Organization
NNTCNS - Non-NATO troop contributing nations
OPSEC - Operational Security
OSIF - Open Source Information
OSINT - Open Source Intelligence
OSO - Open Source Officers
PfP - Partnership for Peace
RFI - Requests for Information
SACEUR - Supreme Allied Commander, Europe
SACLANT - Supreme Allied Commander, Atlantic
SAR - Synthetic Aperture Radar
SC - Strategic Commands
SCI - Science Citation Index
SME - Subject-Matter Experts
SSCI - Social Science Citation Index
STN - Scientific and Technical Network
UN - United Nations
VPN- Virtual Private Network
WEU - Western European Union

FEEDBACK

This manual is intended to be a living document. It represents the first attempt by NATO to place OSINT within the broader context of intelligence efforts. The intention is to subject this publication to regular review and updating to reflect new sources and methods for open source exploitation.

As such, feedback is welcome in any form. Comments, amendments, additions or errors can be reported either with the form below or via email to rsc@saclant.nato.int.

Name: _____

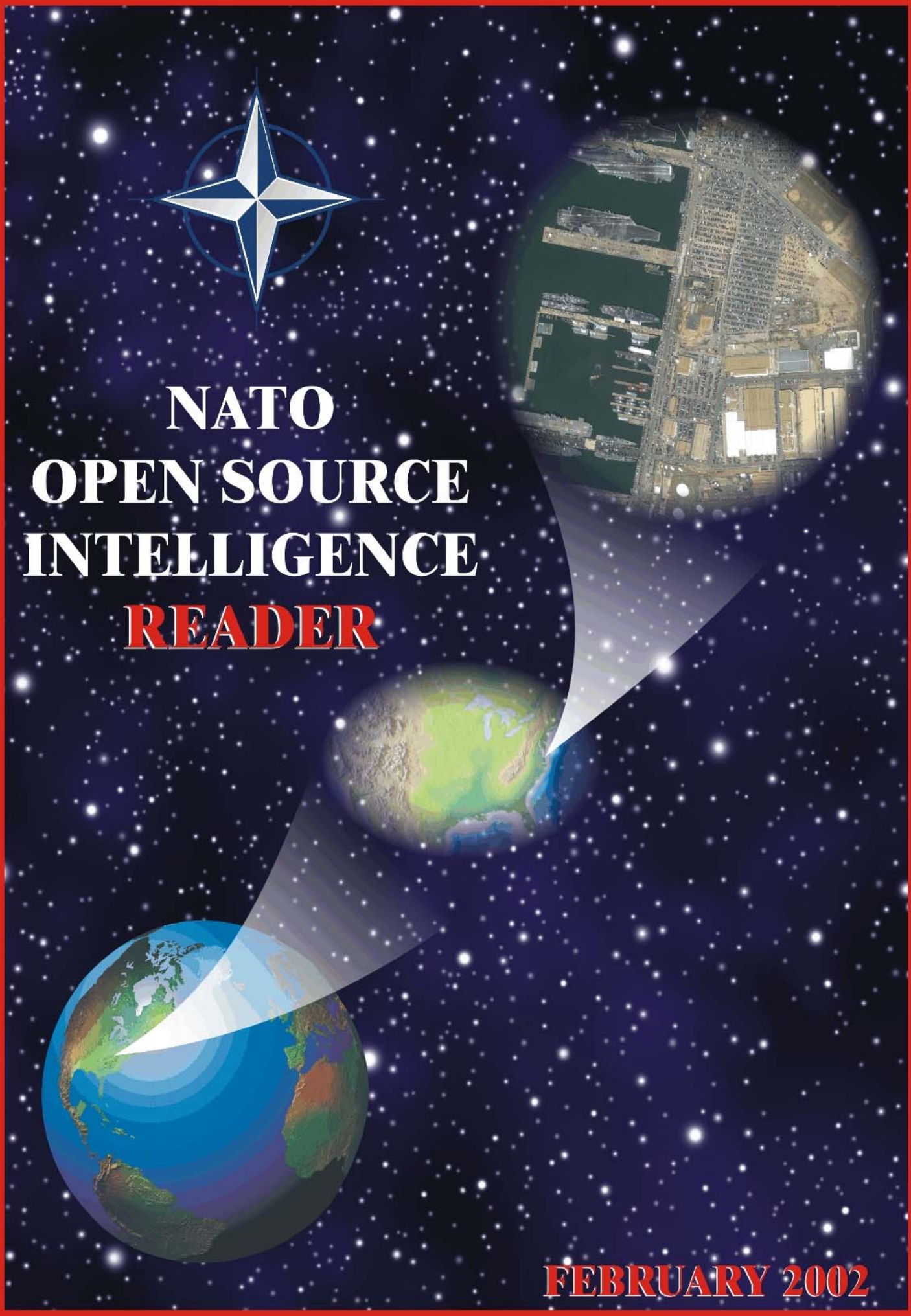
Parent Command: _____

Telephone number: _____

Email address: _____

Comment:

Fax to: HC-310
SACLANT Intelligence Branch
Norfolk, VA
757-445-3572



NATO OPEN SOURCE INTELLIGENCE READER

FEBRUARY 2002

OPEN SOURCE INTELLIGENCE READER

TABLE OF CONTENTS

INTRODUCTION

- Introduction to the NATO OSINT Reader 2
- Open Source Intelligence: The Challenge for NATO 3

THEORY AND HISTORY OF OSINT

- Understanding Open Sources 9
- The Role of Open Sources as the Foundation for Successful All-Source Collection Strategies 12
- Review Essay - Open Source Intelligence 17
- Grey Literature 24

APPLICATION OF OSINT

- Open Source Information 30
- New Risks of Crisis - Fresh Perspectives From Open Source 35
- Secrets For Sale: How Commercial Satellite Imagery Will Change the World 39

INTERNATIONAL VIEWS OF OSINT

- Teaching the Giant to Dance: Contradictions and Opportunities in Open Source Within the Intelligence Community 56
- Open Source Intelligence: What is it? Why is it Important to the Military? 64
- The Privatisation of Intelligence: A Way Forward for European Intelligence Cooperation - "Towards a European Intelligence Policy" 74
- Open Source - Lessons Learned 80
- Optimising Open Source Information Sharing in Australia: Report and Policy Prescription – (Part IV, V) 86
- Open Source Intelligence a 'Force Multiplier' 95

REFERENCES

- Collection and Use of Open-Source Intelligence 98
- Directory of Resources 104

INTRODUCTION

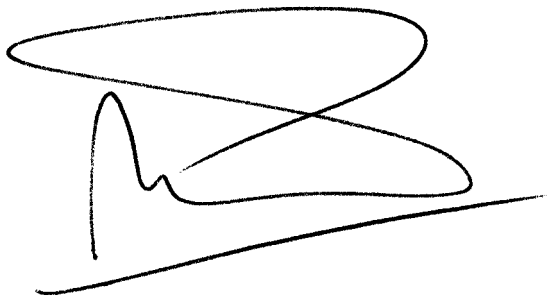
INTRODUCTION TO THE NATO OSINT READER

This publication supplements the *NATO Open Source Intelligence Handbook*, published in November 2001, which provided preliminary information on the subject of Open Source Intelligence (OSINT). The *NATO OSINT Reader,* a focused collection of articles and reference materials by worldwide experts, is designed to give commanders and their staffs the theoretical, historical, practical, and international background necessary to understand how this discipline has evolved. The increasingly robust array of open sources available enables commanders to attempt to satisfy some of their information requirements themselves rather than resorting to directing Requests for Information (RFIs) elsewhere.

The *NATO OSINT Reader* provides comprehensive information and various perspectives on OSINT, including:

- Expositions as to what OSINT is and why it is so important to the military forces of today and tomorrow;
- The theoretical framework of collecting, analyzing, and reporting OSINT information;
- The history of OSINT, particularly as practiced by the NATO nations;
- The application of OSINT to real-world situations both current and future as well as historical;
- International views of OSINT, including but not limited to the views of NATO members; and
- References for further reading and study.

The NATO OSINT Reader has been prepared by the staff of the Supreme Allied Commander, Atlantic, Intelligence Branch in collaboration with staff from the Supreme Allied Command, Europe (SACEUR), and the original sponsor for most of these articles, Open Source Solutions Inc. The *Reader* and the *Handbook* will be supplemented by a third companion document, *Intelligence Exploitation of the Internet*. The information in this trilogy is relevant to all NATO commands, task forces, member nations, civil-military committees and working groups, and such other organizations that may be planning or engaged in combined joint operations.



F. M. P. ’t HART
Rear Admiral, Netherlands Navy
Assistant Chief of Staff, Strategy

OPEN SOURCE INTELLIGENCE: THE CHALLENGE FOR NATO

Commodore Patrick Tyrrell OBE MA LL.B Royal Navy
Commander, Defence Intelligence and Security School, UK
mailto:patricktyrrellrn@cs.com

The dramatic changes in the strategic environment have had profound effects on the way in which NATO conducts its business. Indeed, the changes have altered the very nature of the business in which the Alliance is involved. The most obvious of these is the incorporation of the first three new members of the Alliance for 16 years and the development of the Partnership for Peace initiative. The shift away from the military focus of the Alliance in the days of the Cold War towards a more politically astute and centred organisation was started by Secretary Baker in 1989 when he called upon the Alliance to look towards helping set the new agendas for Europe in the 1990s. At the same time, there have been a proliferation of requirements for intelligence support that are inherently non-traditional; including the readjustment of borders, the study of new migrations, concerns over environmental threats and the need to collect and analyses at the social and economic levels.

Change is never an easy bedfellow and sixteen sovereign nations often have widely differing national interests. The Palmerstonian Doctrine still holds sway in today's strategic environment[1] and the concept of "*realpolitik"* will mean that such national interests will continue to dictate how nations conduct themselves both in private and on the world stage. International organisations like NATO and the UN have provided a forum for nations to be able to develop common approaches to common problems but I still see the attitude of one British Trades Union leader who, during a dispute, was heard to remark: *"I shall negotiate, but never compromise"*. Despite this requirement to achieve consensus and the painfully slow process at times, NATO has made major strides in restructuring and reorganising itself in preparation for the welcoming of new members. There is, however, a clear need to develop a common view of the joint or coalition operating environment if co-operative efforts are to succeed.

One of the most sensitive areas of any military alliance is that of the collection, analysis and dissemination of intelligence. NATO's intelligence structure relies primarily upon intelligence inputs from member nations with only a limited capability, especially in peace-time, for the generation of its own raw data. As such, the NATO intelligence baseline and its standard operating procedures are all centred on a highly classified basis and often exclude unclassified, open sources of intelligence, including commercial imagery.

The concept of an "*information revolution*" has been well developed over the past decade. It is a result of this revolution is that it has allowed us to gain access to unparalleled quantities of data and to retrieve, manipulate, sort, filter, interrogate, digest, plagiarise, and generally bend it to our bidding. Reality is somewhat removed from this in that much of the available

[1] Palmerstone's speech to the House of Commons, 1 March 1848: *"We have no eternal allies, and we have no perpetual enemies. Our interests are eternal, and those interests it is our duty to follow"*

information remains in a format that is not susceptible to digital manipulation, and the search engines are often only as good as the operators who manage them. However, modern technology clearly gives us a tremendously powerful tool with which to conduct information analysis. The revolution has been spurred by the simultaneous collapse of the bi-polar world and the freeing of much data, formerly held as classified. Within this vast "*cyberstore*" of information there will be much that is inaccurate, irrelevant or, simply, out-of-date. It was the veteran US journalist, John Lawton, who in 1995 said: "*It is the irony of the Information Age, that it has given new respectability to uninformed opinion*". It is very tempting to believe that all that scrolls before you on your screen is a quality product!

The revolution, so far, is, essentially, a technical revolution with the development of cheap yet fast computer systems capable of achieving the storage capacities and speeds necessary to search through vast quantities of data. There is, however, a necessary corollary, and that is the development of the human skills necessary to the effective use of the information tools. This is more than the ability to "*surf the net*" and to access on-line databases. It requires an understanding of the subject matter, the techniques relating to computer searches, the ability to make use of an increasing array of sophisticated data-mining techniques, an understanding of where information is likely to be and how to obtain it even if it is not digitally stored in an appropriate database. Perhaps most importantly, the revolution requires dramatic changes in culture, security, and procurement precepts such that the role of the intelligence analyst changes. As the former Deputy Director of Central Intelligence Agency noted at a recent international conference on open source intelligence, the analyst must now "*know who knows*" and be able to identify, task and interact with subject matter experts outside the intelligence community, most of whom do not hold traditional clearances.

Intelligence Skills:

The traditional view of intelligence communities is that they are already aware of the uses (and abuses) of open source material. What has changed, however, is the quantity and quality of available, unclassified material. Many of the skills required of the *information mining engineer* are those already inculcated in the intelligence analyst. The ability to comprehend the overall problem, whether at the tactical or strategic level, is an essential prerequisite for designing an appropriate search policy. The analytical skills allow him to filter the irrelevant, identify the valid and discard the inaccurate. It is important that analysis skills are not considered to be synonymous with searcher or librarian skills, however; the *information miner* must be able to understand where the unclassified information fits into the broad picture. This will demand access to all source data, including where necessary to classified sources. It is this breadth of vision which must be developed if the analyst is not to be myopic in outlook.

Sources of intelligence:

Traditionally, intelligence services have concentrated on classified sources for their analysis. It is true that they have always relied on identifying unclassified sources to provide verisimilitude to the classified product, but the emphasis has remained on the provision of a classified report, issued to those suitably cleared to receive it. In the past, information has been classified either to protect its source or its subject matter. As we approach the millennium, traditional intelligence principles are being turned upside down. As noted by Hugh Smith and cited by Sir David Ramsbotham, "*Intelligence (for coalition and UN operations) will have to be based on information that is collected by overt means, that is, by*

methods that do not threaten the target state or group and do not compromise the integrity or impartiality of the UN (or NATO)".

The development of modern information systems has also made much of the material, formerly only available from classified sources, readily accessible to any who wish to seek for it. Overhead imagery, for example, is now being supplied from commercial sources for a number of non-military tasks including land use, planning, exploration, etc. The resolution of these systems is already good enough for a number of military applications.

Open Source information:

As we have seen, not all the available open source information is conveniently available on interconnected computer systems. Much remains in archives, libraries and other repositories; some is available only on request from government sources and some is in private collections. Availability of information, or at least the ability to access it, is not always international and can only be obtained by someone located in the vicinity of the data. According to US studies, some 80% of what a commander requires, is neither digital in format, in English or, often, unpublished. It will be up to the subject matter expert to bring these inchoate sources into a coherent product.

Open source data is increasingly important to support the intelligence function. The increasing ability to successfully mine data from a large, incoherent series of sources, allows analysts to build up detailed composite pictures of their area of interest. Open source analysis is not a substitute for the traditional classified work, the analyst can use the open source view to be able to ascertain what addition information might be required on a particular subject and, having identified the gaps in his knowledge, task the increasingly scarce resources to target those gaps with whatever tools may be appropriate. Essentially, open sources provide for the foundation for classified collection management, while also providing the context and, importantly from the intelligence perspective, sometimes providing cover for classified sources and methods and often giving evidence as to where new classified studies might be best targeted.

NATO/PfP Requirements:

NATO and the Partners for Peace need to be able to build up a degree of mutual trust and compatibility if the PfP process is to succeed, particularly in the case of Russia. There are few areas as sensitive as the intelligence arena and co-operation in such areas would provide a strong confidence building measure and enhance stability. The new high-level councils, including the recently formed Permanent Joint Council (PJC), will require supporting by a suitable formed intelligence group. Although, as in the past, national intelligence capability can provide an input to individual delegations, the Alliance itself will require independent advice. This can be provided by the existing NATO intelligence staff but would be considerably enhanced if there were to be a NATO/PfP open source facility, working jointly with the existing NATO staffs.

Open Source Programme:

Within the NATO/PfP Open Source Programme, there would be a separate and distinct NATO/PfP Open Source Bureau of modest proportions, specifically tasked with the

acquisition and analysis of information in support of the NATO/PfP secretariats, made up of personnel seconded from all participating nations. There are three potential options:

- establish a "virtual" bureau based on national intelligence staffs operating from their respective national capitals. This is a " Federated Bureau".
- establish a single NATO/PfP bureau at one location fully staffed by a representative group of all member nations. This is a "Central Bureau".
- Composite bureau of nationally based staff with a co-ordination group centrally located. This is a "NATO Web".

The role of the programme, however formed, would be to provide, both on demand and as a routine service, high quality and reliable access to unclassified material. Within the current NATO nations, unclassified material has always been relatively easy to procure. A distinct advantage to NATO will be to have access to those databases and archive which, hitherto, have not been readily available from the PfP nations. The programme would make effective use of existing commercial service providers as well as those of individual member nations. Although the programme will demand highly trained personnel, there is no necessity for the programme to come under the direct control of the intelligence staffs. The intelligence staffs will, undoubtedly, be customers for the product but they will only be one of several potential customers. The bureau will be equipped to handle a wide range of queries, many of which will be easily answered with reference to on-line sources for NATO and PfP staff officers, military headquarters and component commands. Access would be via telephone, fax, and e-mail with clear performance targets to be met. The depth of expertise required will increase depending upon the level of service being provided:

- Periodic awareness service - single page digests on demand
- Search and retrieval - including use of commercial databases
- Primary in-depth research with the identification of appropriate subject matter expertise to meet the customer's requirement
- Strategic forecasting, including that for scientific and technical trends.

The importance of commercial imagery as a foundation for a common operational appreciation cannot be understated. For a relatively modest outlay, commercial imagery could be acquired which would have considerable utility both within NATO and in member nations. The imagery currently available can readily create the 1:50 combat charts which do not exist for much of the region today, as well as providing for the provision of precision munitions targeting information and for three-dimensional, interactive, flight mission rehearsals.

The function of the programme would be to provide what one commentator has described as "*just enough, just in time*" intelligence, clearly focused upon the customer's requirements. It would be designed from the outset to add value to information available to Alliance and national decision makers. In some cases, where the query is complex or the customer is a high priority one, there may be a requirement to provide what would, in commercial terms be an account manager whose task would be to act as an interlocutor between the customer and the programme information staffs. His role would be to assist the customer in focusing his requirements and in the management of the subsequent search and retrieval.

Implementation:

The cost of implementing such a programme is considered to be modest. Much of the required interconnectivity is already in place between the respective capitals and the NATO HQ. The three options would provide for a range of staff costs depending upon whether the programme was set up as a single site entity or as an interconnected, federated system of cells. The advantage of the former is that the members of the programme are clearly linked as a team but the federated solution may allow for better insinuation of the individual open source programme cells with their respective parenting organisation within each nation. This could be augmented by the provision of a co-ordination staff at a convenient site and the use of exchange personnel between the national cells.

There would be a requirement to train the programme staff to a common standard to ensure that all participating nations could contribute fully to the activities of the organisation. Training needs analysis would nee to be done to support not only the initial training requirements but also the longer-term needs of the programme. The DISS at Chicksands in the UK is one of several places where such training could be given.

The provision of such a bureau need not necessarily be a NATO/PfP owned facility: out sourcing of the organisation would save start-up costs and transfer risk to the private sector. The programme would then charge NATO and PfP nations for their services with clear performance criteria laid down for the delivery of the product. This would have the additional advantage of further distancing national intelligence staffs from the provision of the service and, inter alia, allow them to concentrate on their primary functions. It would be important that any selected company would be required to select staff from all participating nations, especially those of the PfP, to ensure the continued national commitment to the overall programme. As an interim alternative, a small contract could be let for the provision of specific open source intelligence products to the NATO/PfP programme. The core value of this programme, however, is the creation of a shared NATO/PfP open source intelligence architecture with interoperable hardware and software. To achieve this ultimate goal, however, will require this programme to be fully integrated into the C4 planning and resource management aspects of NATO and be fully supported by all members of the Alliance.

The key posts in this organisation would be at the senior management level; the director of the programme would have to be chosen for his vision, intellect and management capabilities rather than for the "cut of his cloth". It would be essential that these key personnel had the full support of the NATO/PfP Board. Initially, no more than six full time civilian members are envisioned, with additional staff provided from member nations' military and civilian personnel. Such an Open Source Programme will give a positive, relevant and productive core capability, able to be developed further as the participating nations become more used to sharing information. It will have important implications for future coalition operations whether composed of NATO/PfP or of a wider range of nations. It represents a single, positive step to engender trust, cooperation and confidence between Alliance and PfP members and also gives important skills to their intelligence staffs as we approach the *information millennium*.

Conclusions:

- Open Source programme for NATO is viable option for NATO/PfP

- Open Source programme would provide a significant confidence building measure for PfP nations
- An open source programme will allow PfP and candidate nations to participate at an early stage in the intelligence process within the Alliance
- An open source facility is complementary to existing intelligence functions and will allow the traditional NATO intelligence community to concentrate on other core skills
- The ability to acquire and exploit commercial imagery and external subject matter expertise will assist in the development of a clearer understanding of the joint NATO/PfP operational environment
- Open source analysis uses traditional intelligence analytical skills, although some additional talents are required to ensure effective and rapid retrieval of data
- There would need to be an assessment of the validity of the product
- Training of personnel for such a programme can be easily developed and conducted at a number of places of excellence throughout the Alliance
- The programme would provide 24 hour access to NATO and national staffs with specific "customer" targets established in relation to the delivery of the required analysis
- The entire operation could be undertaken by a commercial provider but the involvement of staff from all member nations would be an important consideration

THEORY AND HISTORY OF OSINT

UNDERSTANDING OPEN SOURCES

Eliot A. Jardines, Open Source Publishing Inc., http://www.osint.org/
Excerpt from "Open Source Exploitation: A Guide For Intelligence Analysts", produced by Open Source Publishing Inc. for the Joint Military Intelligence Training Center (JMITC)

Open Sources Defined

The Intelligence Community has an official definition for open source information. It is contained in a Director of Central Intelligence Directive (DCID) which established the Community Open Source Program Office, effective 1 March 1994. The definition is:

> Open source information for purposes of this directive is publicly available information (i.e., any member of the public could lawfully obtain the information by request or observation), as well as other unclassified information that has limited public distribution or access. Open source information also includes any information that may be used in an unclassified context without compromising national security or intelligence sources and methods. If the information is not publicly available, certain legal requirements relating to collection, retention, and dissemination may apply.(1)

An important subset of open source information is called Grey Literature. The Interagency Grey Literature Working Group (IGLWG) is defined as follows:

> Grey literature, regardless of media, can include, but is not limited to, research reports, technical reports, economic reports, trip reports, working papers, discussion papers, unofficial government documents, proceedings, preprints, research reports, studies, dissertations and theses; trade literature, market surveys, and newsletters. This material cuts across scientific, political, socio-economic, and military disciplines.(2)

Organizations that typically generate the largest quantities of grey literature include: research establishments (laboratories and institutes); national governments; private publishers (pressure groups/political parties); corporations; trade associations/unions; think tanks; and academia. Open source information, then, is acquired from newspapers, television and radio broadcasts, books, reports, journals, and photographs and other images. Of course, these sources have been used successfully in the intelligence production process for many years. What is different now is that there has been an explosion in the quantity and variety of open source material published electronically and readily searchable on-line. The ability to search the World Wide Web or in essence, millions of pages of text within seconds, has proven to be the major impetus for the rise in popularity of open source information as a viable and fruitful component of the all-source process.

Open Sources Quantified

In 1992, during his tenure as Deputy Directory of Central Intelligence, Admiral William O. Studeman reported on the contributions and capabilities of open sources. In an article for the American Intelligence Journal, Admiral Studeman wrote:

> We have identified some 8,000 commercial databases - and the vast majority has potential intelligence value. The number of worldwide periodicals has grown form 70,000 in 1972 to 116,000 last year. The explosion of open source information is most apparent in the Commonwealth of Independent States (ed. The former Soviet Union), where today, there are some 1,700 newspapers that were not published three years ago. FBIS (Foreign Broadcasting Information Service) monitors over 3,500 publications in 55 foreign languages. And each day it collects a half a million words from its field offices around the world and another half a million words from independent contractors in the U.S. - that's equivalent to processing several copies of War and Peace every day.(3)

Open source information is available from a wide variety of sources and presented in a variety of formats. Surprisingly, most of the world's information (some estimates are as high as 80%) remains in printed form stored in libraries or other repositories. Despite the very rapid growth in the quantity and variety of information in electronic formats, the ratio between traditional hardcopy and electronic format information may not be changing significantly because the volume of printed material has also increased in the information age.

Recently, the total quantity of data available on the Internet was estimated to be six terabytes (one terabyte = 1,000 gigabytes).(4) While that may seem to be a tremendous amount of data, a community library containing 300,000 volumes has about 4 terabytes of data. The largest library in the world, the United States Library of Congress has more than 100 million publications. So, while data on the Internet can be searched quickly, the total data available represents only a small percentage of the available open source information. However, the growth of data on the Internet is explosive. A large US telecommunications company has estimated Internet traffic growth at a rate of 30% per month! At that rate, Internet traffic volumes doubles roughly every ten weeks.

It is also important to understand the volatility of Internet data. In a 1997 article, Internet guru Brewster Kahle indicated that the average life of an Internet document was 75 days.(5) Whole Internet sites appear and disappear frequently and without notice. For the open source analyst, this means that any attempts to catalog Internet sites will be difficult and require continuous maintenance to stay current. In short, it may not be enough to simply bookmark Web resources in a browser, effective open source exploitation may require actual archiving of Internet sites.

Contribution Of Open Sources To The All-Source Product

Various attempts have been made to measure the contribution of open sources in the production of finished intelligence. Depending on the topics and the speaker, estimates range from negligible to 80%. Even the most enthusiastic supporters of open sources admit that they are just one of the several sources which support the production of finished intelligence products. One of the most widely quoted descriptions of the role of open sources states:

> Open source intelligence provides the outer pieces of the jigsaw puzzle, without which one can neither begin nor complete the puzzle. But they are not sufficient of themselves. The precious inner pieces of the puzzle, often the most difficult and most expensive to obtain, come from the traditional intelligence disciplines. Open source intelligence is the critical foundation for the all-source intelligence product, but it cannot ever replace the totality of the all-source effort.(6)

Notes:

1. Director of Central Intelligence Directive (DCID) 2/12 effective 1 March 1994. This directive established the Community Open Source Program Office (COSPO) that was charged with development, coordination and oversight of open source efforts throughout the US Intelligence Community. COSPO has recently been reorganized and renamed the Community Open Source Program (COSP) an organization within the Foreign Broadcast Information Service (FBIS).

2. Definition provided by Mr. Bruce Fiene, Executive Secretary, STIC Open Source Subcommittee in a memo dated 15 October 1994.

3. Admiral William O. Studeman, "Teaching the Giant to Dance: Contradictions and Opportunities in Open Source Information within the Intelligence Community" American Intelligence Journal, Spring/Summer 1993, pp. 11-13.

4. Steve Lawrence and C. Lee Giles, "Accessibility of Information on the Web," Nature, July 8, 1999, 107. The authors, both NECI researchers, indicated that as of February 1999, the publicly indexable World Wide Web contained 800 million pages, comprising six trillion bytes of text and three trillion bytes of images.

5. Brewster Kahle, "Preserving the Internet," Scientific American, March 1997, 82.

6. Dr. Joseph Nye, then Chairman, National Intelligence Council, speaking to members of the Security Affairs Support Association at Fort George G. Meade, Maryland, on 24 April 1993.

THE ROLE OF OPEN SOURCES AS THE FOUNDATION FOR SUCCESSFUL ALL-SOURCE COLLECTION STRATEGIES

Mr. Charles Allen, Assistant Director of Central Intelligence for Collection, keynote speaker on Requirements, Collection, and Current Awareness: The Human Dimension

Thank you, Robert, for your kind introduction. I am pleased to be able to address a topic of such importance to the Intelligence Community. The conference program (and Robert's kind introduction) bills me as a "KEYNOTE" speaker. In fact, we all know that, because of the World Wide Web, I am also a "KEY WORD" speaker. My talk will be posted on the Web, subject to key-word retrieval—electronic "pull". Many keywords, by happenstance, will cause this paper to be delivered to the desktops of people who are looking for something entirely different. It serves, however, to point out a problem that the Intelligence Community faces—which all of us face. There is such a volume of open source information that we must rely on information technology to help sort it out, and that technology is quite crude.

For the intelligence analyst, the very richness of open source, and the imprecision of retrieval, pose barriers to effective use of open sources. Compare this to the processes in place for dealing with one of the other intelligence disciplines … or, "INT's." Each of the other INTs has costly and elaborate organic processes that sort out the "signal" from the "noise"—separating the accurate agent report from gossip and invention, separating the real airplane from the plywood decoy.

Take the HUMINT machinery, for example: Analysts and policy makers anticipate their need for information and make those needs known to the HUMINT community—that fabled apparatus of spies and case officers—and by extension to military attaches and to foreign service officers. Overtly and covertly, US Government personnel seek out individuals who possess or have access to the information that will improve US policy making and warn us of hostile intent. The sources, themselves, are often in a good position to sort out wheat from chaff, and the information made available to us by these sources is further refined in the process of drafting reports sent back to Washington. Here in Washington, additional scrutiny is applied before a report is released to the analysts. Disingenuous reports are suspected, vetted, and usually discounted. Repeated interactions with the field, often all the way back to the source, often take place. The bottom line is that knowledgeable humans apply their insights at every stage in the HUMINT process, from initial tasking through the satisfaction of that tasking.

The SIGINT System, too, invests in a costly processing apparatus of human experts to refine requirements and sort out and add value to intercepted information. This quality-assurance overhead is above and beyond the technical machinery needed to make electronic blivots sensible to people. Target by intelligence target, SIGINT analysts laboriously refine mountains of ore to find nuggets of information. A sizeable fraction of the SIGINT System is devoted to winnowing down the raw data so that only the more meaningful information flows to the all-source analysts and policy makers.

Likewise, the Imagery system has elaborate, human-intensive tasking and analytic processes. Imagery-savvy people help the all-source analysts better define their questions and translate them into imagery tasking. And, it is still humans, today, who transform the uncountable, esoteric pixels into meaningful, digestible, pieces of hard information. Still others augment the reports with, annotated, easily understandable pictures ("happy snaps"), which illustrate the points.

But, what about the US Government's open source enterprise? What similar investments do we make? What similar processes do we operate? A knowledgeable audience, you know the answers. Indeed, you probably anticipated the questions. Only for traditional foreign media—newspapers, radio and TV—is there a semblance of a US Government "system" in place. The Foreign Broadcast Information Service, FBIS, is miniscule in comparison to the machinery of the other intelligence collection disciplines. Yet, it provides a service of common concern for the U.S. Government by seeking out, translating, and reporting foreign media information. Proud of its tradition, which prophetically antedated Pearl Harbor, the Foreign Broadcast Information Service advertises its "smart front end"—dedicated human beings with cultural ties to the countries of interest and continuity with the issues. This smart front end has made FBIS a premiere reporter of international events.

However, the distribution media for open sources are changing, the bandwidth increasing and the cost decreasing. By lowering the effective entry cost of publication, new open sources spring up daily and the overall volume is increasing dramatically. It is not clear that the strategy of a human-powered "smart front end" will see us into the future … not clear that it "scales up." To its credit, FBIS is engaging the new technology on its own terms. Whether we are keeping pace or simply falling behind less quickly is an open question. Investment resources for new technology are scarce and the technology cannot yet deliver the precision of selection which we attribute to the experienced human operators.

Having hewn to your conference theme of "the human dimension," and having described what <u>is</u>, I should like to try out on you my ideas about what <u>should be</u>. Then, time permitting, I will close on the advertised topic of "*The Role of Open Sources as the Foundation for Successful All-Source Collection Strategies.*"

The history of how I came to be the Assistant Director of Central Intelligence for Collection is one of spirited negotiation … not so much about Charlie Allen the person …(although modesty permits me to admit there was some of that.) More to the point, there was spirited negotiation about the roles and mission of the ADCI/C, … about the value such a position could add, … indeed, about the very need for such a position.

Many who vied to architect the "New, Improved, Post-Cold-War" Intelligence Community believed we should institutionally reorganize around the "core business processes" of intelligence:

- Collection with attendant Processing; and,
- Analysis and Production.

Or, if wholesale institutional reorganization were more than the system could bear, then, clamored the reinventionists, there should be positions created to embody the management of these core businesses. In the event, Congress created two such positions: the Assistant Director of Central Intelligence for Analysis and Production; and, the Assistant Director of

Central Intelligence for Collection. Not surprisingly, Congress as creator decided these should be confirmatory positions; the Administration was less sure.

Mr. John Gannon serves as ADCI/AP and I serve as ADCI/C. Neither of us has stood for confirmation, but our nominations were made with the advice and consent of the Congress. This is largely a distinction without a difference. Both of us enjoy the strong support of Director Tenet and of the Congress. (About the only difference I can make out, is that you should not refer to me as "The Honorable Charles E. Allen".)

The logic of the proposed reorganization, and ultimately the logic of my position was and is that the collection disciplines—SIGINT, HUMINT, IMAGERY, and to a lesser extent MASINT and Open Source—were perceived as being inward looking. Referred to as "stovepipes", the "INT's" were thought to be collectively less efficient even as they strove to be individually more efficient. The whole was no greater (and perhaps less) than the sum of its parts.

The theorists would say that we were "optimizing locally" as opposed to "optimizing globally" and the changed state of the world to which intelligence speaks is less tolerant of local optimization. Said simply, we can no longer afford the luxury of collection stovepipes given these changes. Principal among the changes, are four that I should like to mention briefly:

- First is the thankful loss of the principal adversary, the Soviet Union, which had the means, and perhaps the motive to devastate the United States.
- Second, and less thankfully, the principal adversary has been replaced with a diversity of asymmetric adversaries, who would challenge us with biological, chemical, and perhaps cyber weaponry.
- Third is the decline in resources allocated to intelligence.
- Fourth is the loss of our collection monopoly in reconnaissance imagery …which, since it is an open source issue, deserves a digression here.

The coming commercial availability of high quality space imagery—coupled with resource constraints on the next generation of U.S. Government imagery satellites—means a potential adversary could access imagery functionally equivalent to that of US forces. For those of us in the U-2 generation, accustomed to an ever more commanding lead in imagery products, this is a watershed event. We may be looking at the culmination of Eisenhower's "open skies" policy … which takes some getting used to. More frightening, we may have reached the point where even dramatic improvements in US Government-unique imagery assets could not alter the equation. Even though we might know <u>everything</u>, the adversary might still know <u>too much</u>. Imagine trying General Swartzkopf's "Hail Mary" left hook in the desert against an imagery-informed adversary.

The *Eminence Grise* of Open Source, our host Robert Steele, is quoted as strongly recommending "… that all managers and analysts take the time to understand what commercial imagery and geospatial data can contribute to their production process. Very high resolution commercial imagery, with processing, is available for only $10.00 to $40.00 a square kilometer. No intelligence product should be regarded as complete until it has considered the possible value-add of commercial imagery."

The US Government may wring its hands about the likelihood that potential adversaries might make better and better use of better and better open sources. However, I suspect many in the audience worry that the US Government, itself, will fail to take advantage of commercial open source offerings. In some ways the Intelligence Community's flirtation with commercial open sources mirrors the broader embrace of commercial, off-the-shelf products by the Department of Defense—an embrace likened to that of two porcupines, who do it very, very carefully.

As a shopper, the US Government is a prisoner of its procurement legacy—a history of monopolizing the market, perceiving its needs to be unique, and reimbursing vendors for costs incurred. This manifests itself in our nit-picking the content of commercial offerings, and our persistent, prurient interest in production cost, rather than market price. If we are to make better use of commercial, off-the-shelf, offerings our motto should be: **adopt, adapt, and stimulate**.

Our first recourse should be to simply adopt from the available offerings those which closely approximate our needs. Or, we should adapt our processes, where possible, to make use of available offerings. Failing that, we should advertise our needs and stimulate vendors to fulfill those needs within their commercial practice.

Some have suggested that each of the Community's components have a "gold team" whose job it would be to advocate, unabashedly, the use of commercial offerings. Another suggestion is aggressive use of "Activity-Based Costing" (ABC), which would show how much each in-house process really costs. This works in tandem with another suggestion, that we take better advantage of Federal Acquisition Regulations (FAR's) which already permit market-price procurement without demanding proprietary cost data.

The glue that holds these suggestions together is an independent estimate of the true worth of a product. We should adopt commercial offerings gleefully if their market price is less than their intrinsic worth to us, and less than the cost of doing it ourselves. (That is why I am committed to develop better measures of effectiveness for all US intelligence collection activities.)

Now, having digressed to establish my *bona fides* as a friend of open source and a champion of commerce, let me return to the job of the ADCI/C and the ostensible topic of my talk: "*The Role of Open Sources as the Foundation for Successful All-Source Collection Strategies.*" Permit me to describe my *Strategic Intent for Intelligence Collection*. The lineage of my vision traces back, directly, to the Director's *Strategic Intent*, which, in turn, flows from the President's *National Security Strategy for a New Century*. Countering the threats to U.S. interests—regional or state-centered threats; transnational threats; spread of dangerous technologies; foreign intelligence inroads in the US; and failed states—the President's *Strategy* stresses, foremost, the need for integrated approaches. In similar vein, Director Tenet's first objective is to "unify the Community through Collaborative Processes."

For my part, the outcomes to which I propose to commit the collection community are to:

- Institutionalize and make routine collaborative cross-INT activities so as to optimize collection resources across disciplines and controlling authorities.
- Enable consumers to express their needs easily and to track the satisfaction of those needs through collection, processing, exploitation, and dissemination.

- Structure an integrated collection system that is sufficiently agile to respond to dynamic needs.
- Maintain balance in attending to short-term and long-term needs and ensure the development of collective capabilities that address long-term needs.
- Rationalize collection resources with bottlenecks in processing, exploitation and dissemination.

As you can see, these preferred outcomes all share the flavor of collaborating, integrating, and optimizing across what have traditionally been collection stovepipes. Open source has always been the backdrop against which the individual INT's play. The first step in formulating a HUMINT strategy against an issue has traditionally been to perform an open source study and assign to open sources as many primary and secondary collection responsibilities for that issue as possible. The SIGINT system, likewise, consumes a prodigious amount of open source as it beavers away, and likewise IMINT uses open sources to set in context its own divinations.

As we look to the future of more tightly coupled collection disciplines, there is every reason to suppose that open sources will provide the matrix about which the other INT's will coalesce. As I have extrapolated from present to future, I am yet humbled by Yogi Berra's commentary about the hazards of prediction, especially about the future. Allow me to reminisce about previous predictions in the open source business.

Five years ago, from a podium like this, at a conference like this, Dr. Markowitz, erstwhile Director of the Community 0pen Source Program 0ffice prophesied that CIA analysts would soon have easy access to the Internet which would make information "… affordable and accessible, but [he worried that] electronic filtering hasn't progressed as far as we'd like." At that same conference, our host Mr. Steele estimated it would take US intelligence agencies five to 10 years to figure out the Internet. More colorfully, he stated that "The CIA is a dinosaur in decline, while the Internet is the future of civilisation." As it turns out, *both* gave timeless prognostications: CIA analysts are still just about to gain universal access to the Internet at large, and electronic filtering still hasn't progressed as far as we'd like. The Internet appears increasingly central to the future of civilization, and …I leave you to decide whether CIA has proven to be a dinosaur in decline.

To close on a grander note, the ultimate test of the President's National Security Strategy is "our success in meeting the fundamental purposes set out in the preamble to the Constitution:

> **…provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity…"**

And this, in turn, will be the final proof of Director Tenet's *Strategic Direction*, my supporting collection strategy, and of the open source contribution to that strategy.

REVIEW ESSAY - OPEN SOURCE INTELLIGENCE

Richard S. Friedman
From PARAMETERS, http://carlisle-www.army.mil/usawc/parameters

> Ninety percent of intelligence comes from open sources. The other ten percent, the clandestine work, is just the more dramatic. The real intelligence hero is Sherlock Holmes, not James Bond.[1] -- Lieutenant General Sam Wilson, USA Ret. former Director, Defense Intelligence Agency

Former Ambassador to Algeria L. Craig Johnstone (presently State Department Director of Resources, Plans and Policy) recently told a Washington conference that during his assignment in Algeria, he bought and installed a satellite dish enabling him to watch CNN so he could have access to global news. He recalled:

> The first week I had it running was the week of the Arab League summit in Algiers and, for whatever reason, the Department was interested in finding out whether Yasser Arafat would attend the summit. No one knew, and the day of the summit Washington was getting more frantic. We in the Embassy were banned from the summit site so there was no way we could find out whether or not Yasser Arafat would show. Finally, at about noon I was home for lunch and watching CNN when the office of the Secretary of State called. The staffer on the other end asked if there was anything at all he could tell the Secretary about Arafat's participation. And just then, on CNN I saw a live picture of Yasser Arafat arriving at the conference. "He is definitely at the conference," I reported. The staffer was ecstatic and went off to tell the Secretary. The next day I received a congratulatory phone call from the NEA bureau for pulling the rabbit out of the hat. How did you find out, they asked? The secret was mine. But I knew then and there that the business of diplomacy had changed, and that the role of embassies, how we do business in the world, also had to change.[2]

Ambassador Johnstone's story provides an example of the value of information from open sources. Allen W. Dulles, when he was Director of Central Intelligence, acknowledged to a congressional committee, "more than 80 percent of intelligence is obtained from open sources." Whether the amount of intelligence coming from open sources is 90 percent, 80 percent, or some other figure, experienced intelligence professionals agree that most *information* processed into finished *intelligence* may be available from open sources. This essay explores the significance of a trend toward increased recognition of the role of open source information and discusses what this may mean for intelligence consumers at every level.

The use of information from open sources (OSINT) for intelligence production is not a new phenomenon. Intelligence services in most nations have always made use of OSINT obtained by working with scholars in academia, debriefing business travelers and tourists, and examining foreign press and broadcast media. Intelligence prepared from sources available to the general public draws from books, periodicals, and other print publications such as catalogues, brochures, pamphlets, and advertisements. Also included are radio and television broadcasts and a more recent technological innovation, the Internet. Collectively, these are frequently referred to as open media resources.

Intelligence--information and analysis that is *not* available to the public--is prepared for use by policymakers and military leaders inside the government. Intelligence is categorized customarily according to the source from which it is obtained. Today, five sources are recognized:

- Reports from human sources (HUMINT)
- Photo imagery, including satellite
- Measurements and signature intelligence: physical attributes of intelligence targets
- Open source intelligence
- Interception of communications and other signals

While most discussions of open source intelligence seem to concentrate on intelligence collection, it is important to view intelligence trends in conjunction with developments in its traditional components. These components are:

• *Costs*. With decreasing national security budgets, government leaders are having to examine their infrastructure. As military forces become more dependent on off-the-shelf commercial technology, intelligence organizations appear headed toward greater reliance on open source intelligence.

• *Sources*. Cost-driven decisions dictate that a significant quantity of intelligence requirements can be filled by a properly designed comprehensive monitoring of open sources, either by the intelligence establishment itself or by private organizations. A particular advantage of open source intelligence is that the product can be maintained at a low level of classification required for these sources and methods. This outcome allows relatively wide dissemination and distribution when compared with material from other sources. This characteristic of open source intelligence is particularly important in coalition operations.

• *Methods*. It has been demonstrated many times that good intelligence production relies on *all-source assessment*. Traditional intelligence structures and methods have been optimized for designated core or central missions, and today many of these remain structured to meet Cold War requirements and scenarios. Current and likely future contingencies seem less likely to involve major hard military net assessments and diplomatic intelligence than was the case between 1945 and 1991. Current and future contingencies probably will continue a trend toward soft analyses of complex socioeconomic, technological, and political problems, and of issues that will include such items as international organized crime, information warfare, peacekeeping operations, and activities associated with special operations and low-intensity conflict.[3]

• *Targets*. Intelligence targets of greatest concern to US leaders have changed since the collapse of the Soviet Union, the accompanying geopolitical upheavals (such as political deterioration in the Balkans), and changes in Western perceptions of global security interests (e.g., the significance of the Middle East). Intelligence agencies must now focus their activities on a far broader range of targets and potential targets than was common in the Cold War era. Today, intelligence professionals have to be concerned with terrorism, major international crime, and arms proliferation, including programs in some areas to produce weapons of mass destruction. They have to be prepared for possible military intervention on short notice in overseas conflicts or for humanitarian relief. Some of these targets require constant scrutiny in substantial depth; for others, broad general surveillance will suffice--provided a reserve or surge capability is maintained.[4]

Although many aspects of intelligence work are changing, for the near term the preponderance of them will probably remain familiar. Today's emerging main problem is

how to deal with new and indistinct boundaries among and between intelligence organizations and functions, and increasing ambiguity in roles and missions. Any intelligence officer who has ever worked at a senior level knows that senior policymakers and government officials abhor ambiguity; they want timely, accurate intelligence. As Peter Schwartz, a recognized futurist, founding member of the Global Business Network, and author of *The Art of the Long View,* told his audience at the Colloquium on the 21st Century, "We will see not only changing rules of the game, but new games. There is an emerging competitive information marketplace in which non-state intelligence will be `cheap, fast, and out of control.'"[5]

Enthusiastic proponents of open source intelligence argue that the information revolution is transforming the bulk of any nation's intelligence requirements and reducing the need to rely upon traditional human and technical means and methods. But Robin W. Winks, distinguished Yale University historian who served in the Office of Strategic Services during World War II and in its successor, the Central Intelligence Agency, concluded, "Research and analysis are at the core of intelligence [Most] `facts' are without meaning; someone must analyze even the most easily obtained data."[6]

The emerging debate between investing in technology and developing competent analysts concerns itself basically with the value and role of open source intelligence. To understand some of the forces that are shaping the debate, we need to weigh the relative benefits of primary and secondary sources, two discrete subsidiary classes of open source material. *Primary* sources, generally taken to include print and electronic media, have always provided information of value to the intelligence community in current intelligence, indications, and warning as well as background information used by analysts in their work. What the so-called information revolution has done is to increase the ability of users to gain access and to manipulate the information, and although most intelligence managers do not believe that the number of primary sources has expanded greatly, the number of *secondary* sources has increased exponentially. To compound the analyst's problem, the objectivity and reliability of many secondary sources are often questionable. We will need more experience before we can accept expansion of secondary sources as a benefit to the management of national security.

The largest general open source collection in the world is the Library of Congress. To replace the original library, which was destroyed during the War of 1812, Congress in 1815 purchased the private library of former President Thomas Jefferson, greatly increasing the collection's size and scope. The Library of Congress now includes works in more than 450 languages and comprises more than 28 million books, periodicals, and pamphlets as well as manuscripts, maps, newspapers, music scores, microfilms, motion pictures, photographs, recordings, prints, and drawings. The library's services also include research and reference facilities, which coordinate with or amplify local and regional library resources.

There are also several thousand databases available from commercial organizations; *LEXIS/NEXIS*, *Dialog*, *Reuters*, and *The New York Times* come to mind.[7] Any discussion of contemporary open sources must now include the Internet and the World Wide Web (WWW). The World Wide Web (developed in 1989) is a collection of files, called Web sites or Web pages, identified by uniform resource locators (URLs). Computer programs called browsers retrieve these files.

The term "Internet" describes the interconnection of computer networks, particularly the global interconnection of government, education, and business computer networks, available

to the public. In early 1996, the Internet connected more than 25 million computers in more than 180 countries.[8] The Internet provides an immense quantity and variety of open source information and must be increasingly looked upon as a source for intelligence purposes.[9]

The Internet and the World Wide Web exemplify technology that is not yet mature. One hallmark of immature technology is an underlying anarchy and a potential for disinformation. In October 1938, when radio broadcasting was emerging as a reliable source of information, producer-director Orson Welles, in his weekly radio show Mercury Theater, presented a dramatization of an 1898 H. G. Wells story, *War of the Worlds*. The broadcast, which purported to be an account of an invasion of earth from outer space, created a panic in which thousands of individuals took to the streets, convinced that Martians had really invaded Earth. Orson Welles later admitted that he had never expected the radio audience to take the story so literally, and that he had learned a lesson in the effectiveness and reach of the new medium in which content was struggling to catch up to technology.

Recent examples with the Internet and its spin-offs suggest that e-mail abuses, careless gossip reported as fact, and the repeated information anarchy of cyberspace have become progressively chaotic. This does not mean that the Internet and the Web cannot be considered seriously for intelligence work, but it does mean that intelligence officers must exercise a vigilant and disciplined approach to any data or information they acquire from on-line sources.

In December 1997, senior officials from Germany, Canada, France, Italy, Japan, Britain, Russia, and the United States (the Group of Eight industrialized nations) gathered in Washington to explore the transnational nature of computerized crime, with specific attention to opportunities for criminals to exploit the Internet's legal vacuum. Among the facts presented to the officials were these:

- Almost 82 million computers worldwide are now connected, according to a Dataquest Market Research Report.
- By 2001 the number of linked computers is expected to reach 268 million.
- The FBI estimated that by 1997, the value of computer crime in the United States had reached $10 billion per year.
- Government agencies are fertile ground for hackers; in 1995 the Pentagon was attacked by hackers 250,000 times, with a 64 percent success rate. The Department of Justice and the Central Intelligence Agency have also been hacked. And the tension over access to Iraqi weapon sites in late 1997 and early 1998 produced a surge of attempts to penetrate US Department of Defense databases.
- The San Francisco-based Computer Security Institute surveyed 536 companies or government agencies, 75 percent of which reported substantial financial losses at the hands of computer criminals.

The principal significance of these facts for the intelligence officer is that Internet sources are subject to manipulation and deception. Consequently, counterintelligence and security processing will henceforth have to include *cyberspace* during analysis.

Perhaps the greatest value to military organizations in this array of adjustments following the end of the Cold War and the proliferation of technologies is freedom from confinement to a fixed geographic site for ready access to basic unclassified references. Modern communications will free deployed military from the need to transport large quantities of

reference material (classified and unclassified) during operations. Military forces in the field can now tap into an immense quantity of information resources in near real-time. Four relevant types are:

- Basic intelligence, such as infrastructure, geography, and order of battle
- Cultural intelligence concerning the society in which the force may be required to operate
- Information of a contextual nature which relates to operational or intelligence message traffic
- Current intelligence reporting concerning the situation in the operational area

Since the quantities of information available are great and much of the information is often irrelevant, staffs of deployed units may find it difficult to use the information productively. Deployed organizations may well have to establish forward and rear intelligence activities. The threat of information warfare will have to be taken into account in planning and executing split-echelon operations.

Providing unclassified information to the general public as well as to officials is the objective of democratic governments in their declarations of open and immediate reporting. Even the tabloid press has never advocated a freedom that would deliberately compromise national security or put the lives of service members at risk, yet there can be unintended consequences from such expanded openness. The British government learned this during the 1982 Falklands campaign when a BBC reporter inadvertently revealed operational plans for what proved to be a costly assault at Goose Green by the Parachute Regiment: the enemy was listening. During Operation Desert Storm, the US government and its coalition partners would encounter other problems. While CNN was reporting directly from the theater of operations, government control of mass communications was in effect in Israel, Jordan, and Saudi Arabia, as it was in Iraq. The sites of SCUD attacks on Israel were quickly cordoned off by the authorities; media representatives were granted access only after a response had been determined by the Israeli government. The state-owned Iraqi media not only repeatedly told its citizens they were winning the struggle, but it manipulated reporting of the use of the Patriot missile against the SCUD, ensuring that CNN and others reported only what the Iraqi government wished. Coalition anti-SCUD measures soon were placed under direct control of Washington.

Intelligence consumers, government officials, and policymakers have not been complaining about a shortage of information; they are suffering from a saturation. The flood of mass-produced data now available and the ensuing overload means that collection is no longer the principal problem. The greater challenge facing intelligence organizations is analysis, consolidation, and timely dispatch of data and results to the individuals who need it. Effectiveness in this process will depend upon allocation of human resources among those responsible for analysis and others responsible for its transmission. An information management executive will consider any increase in volume as proof that information is being managed better, even more efficiently. But the information manager is not in the business of analysis, so he or she is not interested in how well or poorly the information is interpreted, or even if it contains disinformation or inaccuracy. One cannot equate increased throughput to improved situation awareness within a theater of operations.

Nevertheless, the quantitative arguments of information managers recently have become more effective than those of the intelligence community with respect to open source policy.

The last time a similar contention occurred, the proponents of technical intelligence argued that they had the key to ultimate wisdom. As the late Ray Cline, one-time Deputy Director of Intelligence at CIA and later Director of the Department of State's Intelligence and Research Bureau observed:

> The technical miracle has greatly reduced the burden on the secret agent. Lives need not now be risked in gathering facts that can easily be seen by the eye of the camera. . . . Instead the agent concentrates on gathering ideas, plans, and intentions, all carried in the minds of men and to be discovered only from their talk or their written records. Nobody has yet taken a photograph of what goes on inside people's heads. *Espionage is now the guided search for the missing links of information that other sources do not reveal.* It is still an indispensable element in an increasingly complicated business.[10]

Claims of open source enthusiasts need to be examined in context. Those making extravagant claims sometimes have little vested interest in the role and value of open source materials, or even the knowledge or experience to make reliable judgments about the broader issue of multidisciplined all-source analysis by skilled intelligence analysts.

The communications revolution is presenting intelligence organizations with a new challenge far beyond that of mass production. Like other enterprises, intelligence now faces competition from directions believed to have been impossible only a few years ago. As has been true with commerce and industry, intelligence will have to remodel its organization, form new associations, tailor or customize its products, and question its fundamental missions. So long as there are nations led by aggressive totalitarian rulers inclined toward terrorism, or there are fanatics equipped with lethal weapons, democracies will continue to need effective secret services.

NOTES

1. Reported by David Reed, "Aspiring to Spying," *The Washington Times*, 14 November 1997, Regional News, p. 1.

2. Remarks at opening session of the Conference Series on International Affairs in the 21st Century, US State Department, Washington, D.C., 18 November 1997.

3. US military operations in Somalia, Haiti, and Bosnia are examples of requirements of a different nature.

4. It is important to keep in mind an old intelligence maxim: "You can't surge HUMINT!"

5. Address, Washington, D.C., 21 October 1997.

6. Robin W. Winks, *Cloak & Gown: Scholars in the Secret War, 1939-1961* (2d ed.; New Haven, Conn.: Yale Univ. Press, 1996), p. 62.

7. One source estimates the current total to be more than 8000 such databases.

8. The Internet was initially developed in 1973 and linked computer networks at universities and laboratories in the United States. This was done for the US Defense Department's Advanced Research Projects Agency (DARPA). The project was designed to allow various

researchers to communicate directly in connection with their work. It was also developed with the idea in mind that it could provide a nuclear survivable communications system.

9. Current estimates suggest that around 30 million individuals and more than 40,000 networks are connected, numbers which appear to be increasing rapidly. The quantity of data on the Internet is huge. One estimate is total content between two and three terabytes. (A terabyte is a million megabytes.) A typical public library of some 300,000 books has about three terabytes of data. Rajiv Chandrasekaran, "In California, Creating a Web of the Past," *The Washington Post*, 22 September 1996, p. H1. An essay by James Kievit and Steven Metz, "The Internet Strategist: An Assessment of On-line Resources," *Parameters*, 26 (Summer 1996), 130-45, available on the Internet, is an excellent introduction and guide.

10. Ray Cline, "Introduction," in *The Intelligence War* (London: Salamander Press, 1984), p. 8. Emphasis added.

The Reviewer: Colonel Richard S. Friedman (USA Ret.) served in the European, African, and Middle Eastern theaters in World War II as an intelligence NCO in the Office of Strategic Services. After the war, he was commissioned from Army ROTC at the University of Virginia, where he received a law degree. He subsequently served in a variety of intelligence and special forces positions, including an assignment as the senior US intelligence officer at NATO Headquarters in Brussels. Since retiring from the Army, he has worked for the Central Intelligence Agency as a senior analyst, assistant national intelligence officer, and staff operations officer. Colonel Friedman was the lead author of *Advanced Technology Warfare* (1986) and contributed chapters to *The Intelligence War* (1984) and *U.S. War Machine* (1987). As with all *Parameters* articles and reviews, the views expressed herein are those of the author; they do not represent Department of Army policy or that of the Central Intelligence Agency or any other agency of the US government.

GREY LITERATURE

Technical Briefing by Mason H. Soule and R. Paul Ryan
From Defense Technical Information Center, http://www.dtic.mil/

Overview

The Intelligence Community has long taken advantage of the domain of literature offered by the large, worldwide publishing system -- that is, "normal" bookselling channels -- to identify and acquire journals, serials, newspapers, books, databases, and other types of materials that have intelligence value. Analysts combine these so-called open sources with classified materials to provide timely, dependable, and actionable intelligence information to U.S. policy makers and warfighters. Recent changes in political, economic, and even military stances around the world, as well as advances in information technology, have opened up new sources of information that are outside or not yet part of the normal publishing system. One of the Intelligence Community's major challenges today is to acquire and utilize this growing body of "grey information."

The terms "grey literature" and "grey information" are used interchangeably in this technical brief. Traditionally, grey literature denotes hardcopy books and journals, and grey information extends to other types of media. The principal distinguishing feature of grey literature or grey information is that it is outside the normal bookselling channels, which makes it relatively more difficult to identify and acquire than other open source literature. Consequently, the Intelligence Community must devise ways to simulate the awareness and document supply functions that the broader bookselling system already provides, in order to improve its coverage of this type of information. At the same time, it is important to recognize that the resources do not exist to create a duplicate system for grey information.

Scope of Grey Literature

The library science community broadly distinguishes among three kinds of literature:

- "white" or published literature (books and journals, mainly having ISBN or ISSN numbers)
- "ephemeral" literature (items of very short-lived interest such as printed airline schedules)
- "grey" literature, which falls somewhere in between the other two types.

The Intelligence Community developed a definition of grey literature to suit its particular needs, as part of its program to improve its exploitation of open source material. This definition was generated and adopted by the U.S. Government's Interagency Grey Literature Working Group (IGLWG) to support the group's charter of preparing a Grey Information Functional Plan for member agencies inside and outside the Intelligence Community. Building on a Library of Congress definition, the IGLWG distinguished grey literature from other open sources as follows:

> *Grey literature is foreign or domestic open source material that usually is available through specialized channels and may not enter normal channels or systems of publication, distribution, bibliographic control, or acquisition by booksellers or subscription agents*

(Interagency Grey Literature Working Group, "Grey Information Functional Plan," 18 January 1995).

There are many other interpretations of what constitutes grey literature. It remains difficult to define because the boundaries between it and other open source information types vary by user group, and are fuzzy and variable in time and space. But, it is important to those tasked with acquiring this information to have as little ambiguity as possible. Accordingly, the IGLWG included a discussion of the types of information conventionally considered grey. These include, but are not limited to:

- academic papers
- committee reports
- conference papers
- corporate documents
- discussion papers
- dissertations
- government reports
- house journals
- market surveys
- newsletters
- preprints
- proceedings
- research reports
- standards
- technical reports
- theses
- trade literature
- translations
- trip reports
- working papers.

Also as an aid to collectors the IGLWG noted the major kinds of organizations that produce grey literature:

> *"Organizations that typically generate the largest quantities of grey literature include: research establishments (laboratories and institutes); national governments; private publishers (pressure groups/political parties); corporations; trade associations/unions; think tanks; and academia."*

These clarifications are important because they provide guidance to collectors who need to know what kind of information their customers want to obtain. In summary, the key point to make regarding scope is the following. Since grey literature is not well-covered by conventional book trade channels, it is relatively more difficult to identify, acquire, process, and access than conventional open source literature. Hence, if we desire to use grey literature as a source of information, we must be prepared to accept a greater expenditure of resources to collect and process this information in comparison to other open source material.

Problems with Grey Literature

Numerous difficulties arise when analysts attempt to use grey information. Here we mention only a few major ones. First and foremost, grey literature is difficult to search for, identify, and acquire. This puts significantly more burden on the traditional "collection" stage of the intelligence cycle. For example, the only way to learn about or to acquire some trade literature and unpublished conference papers is to attend the functions at which they are made available. Collection networks must identify the event before it takes place, and coordinate attendance and literature acquisition during the event.

Second, open source information already suffers from the problem of a low signal-to-noise ratio, i.e., there are very few nuggets to be sifted from a large body of information. This problem is exacerbated in the grey literature domain because thousands of organizations generate literature, while only a fraction of these producers and their products are of interest to the Intelligence Community. The situation worsens daily as the availability of information from myriad Internet sites increases.

Third, grey literature is more difficult to process than other open source types because of its predominantly nonstandard formats. Product brochures, for example, rarely provide adequate information to allow them to be catalogued or retrieved easily. Important information, such as author, title, place and date of publication, and publisher, often is lacking from other grey literature types, as well. In addition, much grey information remains available only in hard copy. Although this is changing as Internet distribution expands, the absence of standards and keyword indexing will make it difficult to find information on this electronic forum with other than direct character matches.

Fourth, grey literature varies radically in quality since it often is unrefereed. Integrity is an issue with Internet data, as well, since electronic data are easy to alter.

Finally, foreign grey materials, which are the main interest of the Intelligence Community, are often not in English. This places additional burden on the processing system which needs human or machine translators to translate the material for the user.

Importance of Grey Literature

Key reasons for distinguishing grey literature from other open source materials lie not in the problems it generates but in the value it provides. The Intelligence Community's interest in open source literature stems from its potential to contain information of intelligence value and which may be obtained cheaper, faster, and at a lower level of classification than information acquired through other intelligence collection channels. As a subset of open source, grey information has certain other attributes, as well.

1. It can provide information that often is unavailable in published open sources. Many brochures and the information they contain never will appear in a published version.
2. It often is available on a more timely basis than conventional literature. Conference papers, for example, are available long before any follow-on, published article will appear, yet the information content of the two versions may not differ significantly.
3. It can corroborate important assertions found in other sources, which is always paramount in intelligence analysis.
4. It may have a concise, focused, and detailed content. This is particularly true of technical reports and unofficial government documents, whose information content will be greatly reduced in the published form.
5. It is becoming a common means of information exchange, particularly as personal publishing software improves and Internet access expands.

For all these reasons, grey literature must be part of an overall awareness strategy that requires a thorough search be made of all available open sources in the quest to provide answers to intelligence questions.

Federal Government Initiatives to Address Grey Literature

The successful exploitation of grey literature requires coordination and sharing of knowledge by all involved parties to reduce average unit costs of grey literature. Recognizing this, in February 1993, the Director of the Foreign Broadcast Information Service (D/FBIS) asked for IC and non-IC participation to develop a functional plan for acquiring, processing, and disseminating grey information throughout the IC. In response to that call, representatives from the Armed Forces Medical Intelligence Center (AFMIC), Army Materiel Command (AMC), Community Open Source Program Office (COSPO), Defense Intelligence Agency (DIA), Defense Technical Information Center (DTIC), Department of the Army (DA), Department of Energy (DOE), Library of Congress, National Air Intelligence Center (NAIC), National Ground Intelligence Center (NGIC), National Security Agency (NSA), National Aeronautics and Space Administration (NASA), and National Technical Information Center (NTIS), met with FBIS and other CIA Headquarters components to form the Interagency Grey Literature Working Group (IGLWG).

The Grey Information Functional Plan created by this group was approved by D/FBIS and D/COSPO and released in January, 1995. It addresses issues of acquisition, processing, and dissemination. The plan lists ten key findings that represent the basic precepts for action to make grey information available to help fulfill intelligence needs in the 1990s:

- Develop an *awareness* of the availability of grey information within or to organizations as a means of minimizing acquisition and processing costs to other agencies.
- Improve IC *cooperation and coordination* with key non-IC members that currently collect the majority of grey information materials to maximize its availability and to reduce duplicate acquisition.
- Implement *needs driven acquisition* of grey information to better manage acquisition costs.
- Identify and assign *areas of responsibility* among Government agencies to cover myriad subject areas on a worldwide basis with a dwindling resource base.
- Provide *timely notification* of the availability of relevant grey information.
- Utilize a *tiered processing approach* -- driven by user requests -- to minimize total processing costs.
- Institute *long-term storage and retrieval* systems.
- Leverage *existing U.S. Government capabilities for deposit and distribution* to reduce infrastructure costs.
- Incorporate advancements in *enabling exploitation technologies* (principally optical character recognition, machine translation, and machine-aided indexing) to improve processing.
- Employ credible *management metrics* to ensure the continuing effectiveness and efficiency of systems and processes.

The IGLWG believes that grey information can be better harnessed to satisfy intelligence needs if we can carefully implement these basic ideas among acquisition agencies and wisely use existing Government processing and distribution functions.

Members of the IGLWG have been involved in other ways to improve access to grey literature, both as individual organizations and as part of multiagency ventures. Over the past five years, first NASA and later FBIS, NAIC, DTIC, and COSPO have co-sponsored the

annual International Acquisitions Workshop to share knowledge of grey and other open source collections and acquisition methodologies among Government information specialists. Under a COSPO-funded project, NAIC developed a Grey Literature On-Line Catalog (GLOC), a database residing on the CIRC system which describes the grey literature holdings of many Government and non-Government information centers. FBIS has developed a Grey Literature Tracking Database, which describes important FBIS grey literature acquisitions as they are made available. NTIS has actively collected and made available many foreign technical reports, including a large collection of South Korean studies. The Library of Congress is working to make more Japanese grey literature available to its users. And DTIC has been working with the British Library Document Supply Centre (BLDSC) to provide access to the latter's excellent collection of conference papers and proceedings. All of these activities could benefit from the broader participation of other Government agencies on the IGLWG.

Role for Information Technologies in Processing Grey Literature

The initial summit conference and this e-journal version of the proceedings are excellent forums for the present paper because many dimensions of grey literature exploitation could benefit greatly from the infusion of Information Technologies (IT). We discuss a few ways that grey literature exploitation can be improved in the areas of acquisition, processing, dissemination, and analysis.

Acquisition

The low signal-to-noise ratio of grey literature necessitates that identification and acquisition be considered as separate steps in the collection phase, because a vacuum cleaner approach is not possible with grey literature. Acquisition instead must be demand-driven. Help is needed from the IT to relate grey literature availability to user requirements, as well as to share awareness of interagency holdings to reduce duplicate acquisitions.

Processing

Much ongoing work in the Government is aimed at improving scanning, machine-aided indexing, optical character recognition, and machine translation, which will benefit all open source exploitation. In grey literature, a tiered processing system needs to be designed so that resources commensurate with the demand for a grey literature product are expended on its processing.

Dissemination

This is not generally an issue with grey literature since its real difficulties stem from its acquisition and processing. Still, issues of copyright and electronic document dissemination are important. The size of some technical reports make them harder to transmit or store electronically, while copyright becomes a nightmare as thousands of producers must be tracked down for royalty purposes.

Use

As with processing, much work is ongoing to provide the analyst with tools to analyze digital information. Metrics are needed to evaluate the cost effectiveness of grey literature as a

marginal source of intelligence. If it is not providing significant value, then acquisition and processing methodologies must be rethought.

Conclusions

To improve analyst and information provider efforts to find grey information, we must understand what role grey information can play in solving open source intelligence issues. It is somewhat -- but not entirely -- artificial to think of grey information separately from open source since grey information is a subset of the latter. It is important, however, to know how to use grey information within this broader open source context. One must first exploit what is possible from easier-to-obtain open sources before using possibly marginal sources from the harder-to-obtain grey information domain. However, this cost reduction must be balanced against the benefit of the more timely availability of some grey literature products. Analysts must think about how grey information contributes to meeting their information needs and in what subject areas it is most advantageous or productive. Analysts then must provide feedback to the information providers who serve them.

A brief biographical notation

About Mason H. Soule: Mason Soule is a Research Scientist in the Systems Analysis and Engineering Department of the National Security Division at Battelle Memorial Institute in Columbus, Ohio. His Internet address is mailto:soule@battelle.org.

About R. Paul Ryan: Mr. R. Paul Ryan became the Deputy Administrator of the Defense Technical Information Center (DTIC) in July 1989. DTIC is the central source within the Department of Defense (DoD) for acquiring, storing, retrieving and disseminating scientific and technical information (STI) to support the management and conduct of DoD research, development, engineering and studies programs.

In previous positions at DTIC, Mr. Ryan was Director, Office of User Services and Marketing. He was responsible for developing and implementing a marketing program, product management program and improved user services for DTIC. The Office acts as the liaison between DTIC and its user community; manages several regional offices (Albuquerque, Boston, Dayton, Los Angeles); provides training and support to the Defense RDT&E; Online System (DROLS), and the Department of Defense Gateway Information System (DGIS); manages such special programs as the Small Business Innovation Research (SBIR) program; the Historically Black Colleges and Universities (HBCU) program and the University Research Support (URS) program; and is responsible for the annual users conference and regional meetings held each year.

APPLICATION OF OSINT

OPEN SOURCE INFORMATION

John W. Davis
Originally published in ARMY Magazine, July 1997

Imagine the horror of death by friendly fire. See the faces of a mother and father at the moment they are told their son or daughter was killed by American fire. Today, far more than bullets can cause this horrific scene. This is a new age, and there are new threats.

Information warfare is the latest theme to capture the imagination of the US Army. Force XXI, the technological army with the narrow soldier base, depends on the rapid and accurate flow of information to fuel its highly technical killing power. To protect its classified information, this army can depend on traditional security elements. This new army, however, also generates a massive amount of unclassified material that is overlooked by traditional security measures. Could this material reveal the secrets the Army hopes to protect? In the information revolution, "open source" information is the wild card of the modern battlefield. It is a form of friendly fire. The Army must protect this vulnerability through operations security.

Information - its access, use, analysis and control - is clearly a military matter. Classified information is protected by an array of security measures that are well known and practiced. But what about the literally millions of bits of unclassified personnel, logistical, operational and supply documents that Force XXI is generating? What can this information reveal and who will watch over it? What will protect this information from the silent, listening collector who is picking up the information that spews out over unsecured faxes, mail messages and telephone networks?

The Army must ask itself if this is a problem. Can the flow of information necessary to conduct operations hurt the Service? What if the unclassified material is so voluminous, so comprehensive, that it reveals the essential secrets the Army is otherwise so careful to protect?

At the beginning of World War II, some 300 British engineers died because they could not defuse the new electrical bombs dropped by the Germans over England. It took trial and error and the chance discovery of intact electrical bombs on a downed German aircraft before the technology was defeated.

Eight years earlier, in 1932, the technology for such bombs had been entered into the public records of the British patent office, yet none of the engineers knew about this open source information.

Three hundred men died while the answer they sought gathered dust in an unlikely place. Those who built the bombs that killed these men had found the information first and laid claim to it legally and openly. Had they known this, it would have been easy to convince the British people of the value of open source awareness.

An earlier example involves the Maxim gun. When asked in 1884 why Western nations had colonized almost the entire known world, the English writer Hilaire Belloc said that it was not because of their advanced civilization, greater universities or cultural advances.

No, he quipped, "Whatever happens, we have the Maxim gun, and they have not." Of course, the technology for this early machine gun and other technological information was routinely shared and sold in open contracts between "civilized" countries. In World War I this exchange of information resulted in the slaughter of an entire generation; by then all nations had access to the Maxim gun.

These stories show how open source information works. What is routinely, even inadvertently given away today could kill someone tomorrow. Information that is not tracked could later surprise the Army on the battlefield. These stories about open source information end in bloodshed. Is it inappropriate to say that the victims died from friendly fire?

Information is the lifeblood of the high-technology Force XXI. An array of information will deploy with Force XXI wherever it goes, whoever the adversary is. Unlike most of the adversaries of the United States, whose technological developments are not shared openly, much of the information about Force XXI's development is available to the entire world. For example, the Associated Press reported on a Pentagon armaments display showing soldiers with heat-sensitive night-vision sights, lightweight body armor and computer backpacks. They reported concepts about laser warplanes, seagoing missiles and more. Today there are many armaments magazines, defense sites on the Internet and newspapers reporting the business of warfare. These open sources of information are cheap, readily accessible and accurate.

Through the eyes of a western analyst, the publications are what they seem: military trade journals that cover market share, sales opportunities, competitive and joint ventures, and national acquisition goals. They are straightforward.

Graphs and computer-generated art enhance the stories and illustrate the concepts. In the photographs used, sleek missiles fly, spotless armored vehicles roll and wholesome, clean soldiers pose with the latest weaponry in pleasant pastures. There is no blood.

Consider now the reader of this same information from poorer, less industrialized, embargoed or other-wise ostracized nations. Consider also the people of para-nations, the ethnic clans, narcotics traffickers and terrorists. They see the same information in terms of life or death choices. They cannot afford technical research or development, and they cannot "comparison shop." They know they must choose wisely the first time because there may not be a second choice. For them, the only collection method may be what they can learn from open publications. The more sophisticated groups can build on information from open sources and confirm their conclusions with traditional collection methods. Their interest is far from abstract.

Several truisms must be accepted in this new world of half-wars against nontraditional adversaries. Poorer nations want to survive. In order to do so they are offered the Hobson's choice of spending what wealth they have on arms or relying on a guardian nation to arm their people. They are not interested in future sales, in market share or in the bottom line. If they do not choose correctly from the arms necessary to protect themselves, they will cease to

exist, or worse, be enslaved. Obviously, they see the world from a dramatically different perspective.

The West views military technology as a chess game. One player creates this, the opponent creates that to counter it, and so on. In this rational game of give and take, no one dies and the game goes on. Some call this the arms race, but nobody dies in a race. Such a sterile view of the industry misses the point.

Analysts of arms markets from non-Western countries or para-nations see the armaments industry differently, and arguably more clearly than Western nations do. They, like the United States, will determine their needs and do all within their power and budget to acquire those necessities. Unlike the United States, they see their existence as often nasty, brutish and short. They often feel they must confront the killer at the door, rather than the economic competitor in the pin-striped suit. It is not surprising that poorer countries decided to buy machine guns as soon as they could afford them, once they saw what happened to those who did not.

They are doing the same thing today, and have a vested interest in what is available on the arms market and in how their potential adversary will fight. What if their potential adversary is the United States?

These poorer countries want to know, simply put, how to beat the United States in battle. To be able to surprise the US military, they will try to learn more about it than the military knows about itself. They do not have the wherewithal to conduct massive technical research, so they will take any shortcut. All open sources will be exploited. Why spend the money on research and development if the final product is going to be for sale or is explained on the Internet? Why test weapons if the answers nations seek are printed in publications that cost only a few dollars each? Comparison tests will be done by those governments that see weaponry more as a commodity to be marketed than as a means of killing people.

Western powers think of long-term strategies while poorer nations wonder how to stop the immediate threat. They know they are dead if they make the wrong choices, so they research information thoroughly. If they can piece together information about the true intentions of an adversary from what they can collect on the open source market, they will do so. It may be the only source they have. These are the types of adversaries the US military will confront tomorrow.

These differing perceptions of the world - one of the rich nations, the other by poor - must be better understood. A poor man does not care about higher technology tomorrow if his weapon will surprise his enemy today. To achieve this, he may act in a way contrary to what the West considers to be in his best, rational interest. Westerners must see the world with new eyes - their potential adversary's eyes. History offers many examples.

In the 1920s, for instance, a beaten Germany, penned in by the Treaty of Versailles, entered joint ventures with Bofors Corp. of neutral Sweden. The Germans had studied the published armament policies of other European nations and had observed the soldiers occupying their country. They had studied what would win on a future battlefield, then set out to get it in any way they could.

Before World War II, Germany illegally trained its army on the land of its arch-rival, the Soviet Union. Despite open reports of Germany's illicit training, other nations were too complacent to challenge this threat. The West was thinking about long-term, rational arms races. Germany was thinking about a blitzkrieg.

In the later example, the Unites States was shocked when it was revealed that the Vietnamese communists had routinely spliced into U. S. telephone lines. Open communications were compromised. These were simple farmers who should not have had the capability, the United States complained. The nation did not see the world through its adversary's eyes.

Today, are the Bosnian Muslims going to rely on the Unites States to take action against a vengeful Servia, or will they take their own measures? Does anyone doubt that they are devouring every statement and operational move made by the U. S. Army in the Balkans?

Every document, every communication made by the U. S. military's Balkan-deployed soldiers is subject to collection. Seemingly innocent communications could confirm or deny the fears of the many groups involved in Bosnia. How many American soldiers realize that a TDY order, supply form or logistical document could betray the military's true intentions? Open source information takes this operational release of information even farther.

Westerners may see no great loss when technology is compromised because they may never see the battle field of their work. They may think abstractly of their product as a funded program, not as something that kills someone. Their counterparts in another, less powerful country would face imprisonment or execution if they compromised hard-gathered information.

Westerners must "publish or perish." They have a "right to know" and a free and inquisitive press. Non-Western counterparts do not. The arms race fuels the West's ever expanding market and the information-rich marketing ethic that advertises it. The military must create policies that protect all its information - even the unclassified - because, in this new world, information that kills soldiers is a commodity available for sale.

Operations security, a process of securing this unclassified information, can protect Force XXI. The security process is simple. Each element of the Army must ask itself, "What is it that I must protect, or else I'll fail in my mission?" The answer is that critical information must be protected, as Sun Tsu noticed so long ago. Not everything that can compromise a mission is classified.

Next, the collection threat to this information must be studied. Soldiers must consider who wants what they have. Here, the intelligence community can provide assistance. The collection capability could be a highly sophisticated process or a hacker who can read the Army's e-mail. In weighing the threat to the critical information, the answer to the next question, "Is the Army vulnerable?" may be surprising. Even units with 100 percent traditional security of their classified information have been compromised by a hemorrhage of unclassified data. Unit leaders did not tell their soldiers what was critical to protect, and soldiers did not control bar talk, telephone talk or what went out over the wire, much less what went into the trash. After the risks are weighed, such as collection capabilities and reaction times, countermeasures must be decided on.

The Army must communicate to accomplish any mission, but it has to remain aware of the unseen listener. Soldiers must know what an adversary can do. To survive, other countries will read everything the Army writes and listen to any conversation they can. The Army has to see itself as others see it.

Once they learned that the Viet Cong had made tiny mines from discarded C-ration cans, soldiers stopped leaving cans uncontrolled. Now, the Army should do no less with its open source information.

NEW RISKS OF CRISIS - FRESH PERSPECTIVES FROM OPEN SOURCE

Dr Brian Rotheray, BBC Monitoring – 2001
Copyright BBC, http://www.monitor.bbc.co.uk/

OPEN SOURCE

An early British open-source handbook tells the story of a general sent to subdue an island. This island had recently been partially occupied and was in revolt. The general succeeded. He was an imaginative and decisive officer and he made extensive use of the various forms of intelligence.

He sent out ships to chart the island's coast and identify its harbours and waterways - ***naval intelligence***. He surveyed the interior - ***mapping*** and ***imagery***. He studied the weapons of the local rebels and their tactics and devised his own methods to counter them - ***military intelligence***. When it suited, he made deliberately slow progress through the country, allowing his reputation to go ahead of him - ***media spin***. He investigated the state of agriculture and industry, identified mineral deposits and mining potential and established that the country was worth occupying - ***economic intelligence***. He had reported to him the speeches of rebel leaders and so heard their arguments and knew what they said about him - ***political intelligence*** and ***open source***. (Some speeches are fully texted in the book.) And he studied the locals. He found out about their languages and religion and character and "he listened to the experts" - ***cultural intelligence***. He learned what made the people tick, particularly that "little was accomplished by force if injustice followed", and after winning he governed accordingly.

This is not a recent book and it is about the British, not by them. It is by the historian Tacitus and is the biography of his father-in-law Gaius Julius Agricola, who subdued Britain for the Romans two thousand years ago. Plenty of sand has run through the glass since then, but the same basic ideas apply.

Monitoring the media is as old the media. Former German Chancellor Helmut Schmidt is supposed to have said that he got more out of reading the *Neue Zuericher Zeitung* - a Swiss daily newspaper - than out of all his intelligence briefings. Part of the humour of this is that the *Neue Zuericher* looks like an old fashioned "intelligencer" with the style of an eighteenth-century broadsheet.

All countries and governments practise media monitoring in some form or another From the Japanese embassy in London monitoring the UK press, through the mighty German Chancellor's press office, via companies that track mentions of toothpaste manufacturers - and the like - on local music stations, to the great spin-doctoring concerns that influence every move a politician makes. Governments, parties, interest groups, transnationals - they are all at it.

The BBC is a major broadcaster domestically within the United Kingdom and internationally. It employs around 22,000 staff, runs a number of national and international television channels, five national and around 40 local radio channels. In addition, BBC World Service radio broadcasts in 40 languages and has around 150 million listeners. There is also a major

commitment to Internet services, including BBC News online – one of the world's best-known.

Since 1939, the BBC has found it worthwhile to monitor other broadcasters – other media – around the world and it continues to support a unit to do this. The BBC does this to understand its markets and competition and to help it report the news to those markets.

The BBC also sees its monitoring service as a national asset supporting British interests. Our reporting helps inform a British and world public and deepens public understanding about what is going on in the world and why. It is a service to the British government, civil service and institutions. In effect BBC Monitoring sees open source media reporting as helping a number of communities of interest:

- the diplomatic community – and the wider community of those interested in foreign affairs;
- the defence and intelligence – and law-enforcement – communities;
- the fourth estate – broadcasters and other media – and through them the British and international public;
- the legislature – parliament and its members;
- also the educational and the business communities;
- and what is described in Britain as "joined-up government" – the bits that aim to make the individual elements act as a coherent whole. In practice that means the Prime Minister's own offices.

All these "communities", these types of organisation, can benefit from knowing what is appearing in the media around the world. And there are three types of benefit that an organisation like BBC Monitoring can offer:

1. Individual reports - many hundreds a day about what is happening in the world - information
2. A picture of what people and the media in a country or region are saying - opinion
3. Knowledge management – assistance in wading through millions of words in numerous languages from almost innumerable media sources and making some sense out of them

The valued-added help in data **navigation** comes from:

- knowledge of countries, languages and cultures,
- knowledge of the sources and media environment
- knowledge of the customer's needs and tools, as well as human skill to deliver the right material to suit the right function in a given situation.

BBC Monitoring's aim is to provide sustained global coverage, maintaining a wide overview of foreign media source and monitoring the key ones.

This means not **just radio and television,** but also news **agencies** and the **press** and the **Internet.**

Working in partnership with FBIS, BBC Monitoring offers output from the monitoring of around 3,000 sources in 150 countries and from 100 languages. What is offered is the product of a high level of skill and understanding.

BBC Monitoring provides global coverage through its close partnership with FBIS - the US Foreign Broadcast Information Service. The partnership works through a division of coverage and by working to similar operational and editorial standards. Each partner passes the other its monitored output - the transcripts; each partner turns these transcripts into products and services for its respective customers.

FBIS provides coverage of the Far East and Latin America The partners share coverage of Africa, the Middle East and Europe. BBC Monitoring majors in the FSU and Central Asia Both partners maintain a string of monitoring operations to cover their areas.

BBC Monitoring's key trademark is that it tells you **"the words as spoken"** - exactly what a television service is reporting, exactly what a minister says in an interview, exactly what a treaty contains.

Around 800 reports are issued each day. Reports like these can be accessed through Internet databases, profiled directly to end-users or fed into user organisations' intranets.

Thousands of words and more than words. Also pictures, sound, information about the make up of governments and other official organisations.

It is important that thus is also a service - not just a machine. At the highest level of service the users get desk-to-desk contact with the monitors who know the target countries and the topical issues.

BBC Monitoring is aiming to provide effective open source intelligence - to help cover the needs of different functions in different situations at different times that add up to a strikingly coherent overall need. Our target: to collect **the right information,** make it **plain,** and deliver it to the **right place** at the **right time.** In conclusion, a short open source “entertainment” from the archives:

DON'T IGNORE THE OBVIOUS [with apologies to James Thurber]

The goose family - father goose, mother goose and daughter goose - is sitting at home minding its business. Suddenly there is a ring at the door.

“Aha,” says daughter goose. “No doubt it is a young gentleman caller for me!”

“Forget it, honey,” says father goose. “I'm expecting a brush salesman come to sell me a brush. I'll open up”

Mother goose - more careful - looks out the window and sees a large, hungry-looking wolf with sharp teeth and a bushy tail

“It's a wolf,” she says. “Got wolf written all over him. Teeth and a big tail. Don't open the door.”

“Don't be silly, honey,” says father goose, not bothering to look. “There's no wolf activity round here. There's a bunch of guys working undercover on wolves. They'd warn us if there was anything going down. It's the brush salesman What you think are teeth are its business cards. What you think is the tail is my brush. "

So he opened the door - and the wolf ate him up.

The moral: What's open source for the goose may not be open source for the gander.

SECRETS FOR SALE:
HOW COMMERCIAL SATELLITE IMAGERY WILL CHANGE THE WORLD

Yahya A. Dehqanzada and Ann M. Florini
Excerpts from "Secrets for Sale: How Commercial Satellite Imagery Will Change the World" reprinted by permission of the publisher (Washington, D.C.: Carnegie Endowment for International Peace, 2000)

EXECUTIVE SUMMARY

By the year 2003 at least eleven private companies from five different countries expect to have high-resolution commercial remote sensing satellites in orbit. These new satellites have capabilities approaching those of military spy satellites, but with one key difference: their images will generally be available to anyone able to pay for them. This new technology raises a host of policy concerns with which governments, business executives, and analysts around the world are just beginning to grapple. This monograph, inspired by the discussions at a recent conference of the Carnegie Endowment for International Peace, addresses those policy concerns(1).

Key conclusions are that:

Increased access to high-resolution satellite imagery will shift power from the former holders of secrets to the newly informed. Governments that previously had limited or no access to satellite imagery can for the first time see what elite states have observed from the skies for many years. In addition, commercial satellite imagery will provide an independent source of information to groups in civil society. Both state and non-state actors will employ satellite imagery to monitor and sometimes publicize the activities of various countries and corporations.

High-resolution satellite imagery has both beneficial and malign applications. It can significantly enhance the ability of governmental and nongovernmental organizations to respond quickly to sudden humanitarian emergencies such as in Somalia and Iraq, document and publicize large-scale humanitarian atrocities such as those witnessed in Kosovo and Rwanda, help control environmental problems ranging from impending droughts to deforestation, monitor compliance with international agreements, and assist in managing international disputes before they escalate to full-scale interstate wars. But abundance of information does not guarantee benevolent uses. State and non-state actors could employ remote sensing imagery to conduct industrial espionage, collect intelligence, plan terrorist attacks, or mount offensive military operations.

Attempts to control access to high resolution satellite imagery are bound to fail. Since the end of the cold war, technological progress, coupled with a greater appreciation for the military, civilian, and commercial utility of high-resolution satellite data, has persuaded governments and corporations in virtually every region of the world to invest in indigenous remote sensing industries. As a result, both the satellite technology and the necessary support infrastructure have become global. It is unlikely that any one country, regardless of its size or market share, can by itself curb access to high-resolution satellite imagery. And because of the large number and varied political agendas of the countries that will operate various

satellites (Canada, France, India, Israel, Russia, the United States, and possibly China), multilateral agreements on control seem elusive. Governments need to accept this new era of mutual assured observation, take advantage of its positive effects, and find ways to manage its negative consequences.

Commercially available high-resolution satellite imagery will trigger the development of more robust denial and deception and antisatellite countermeasures. Widely available high-resolution satellite imagery will undoubtedly compel governments to develop effective means for keeping their secrets hidden. Many states, especially those with regional adversaries, will invest heavily in denial and deception and antisatellite countermeasures. Such a development could have serious implications for confidence-building and crisis management among mutually vulnerable states.

Expected gains from commercial high-resolution satellite imagery may be exaggerated. Satellite imagery is only one source of data among many. While it can detect large-scale troop movements, mass graves, and deforestation, it cannot reveal what those troops' intentions are, who is buried in the mass graves, or how deforestation can be stopped. Complementary data are necessary to turn satellite imagery into usable information.

Good training for imagery analysts is essential. Satellite imagery can be difficult to interpret. It takes years before an analyst gains the experience and expertise necessary to be able to derive useful information from gigabytes of transmitted data. Junior analysts are wrong far more often than they are right. It is essential that imagery analysts go through extensive training not only at the beginning of their careers, but also every time they shift the focus of their work—analysts who specialize in interpreting and analyzing the activities of ground forces cannot overnight become experts on nuclear testing or environmental issues.

INTRODUCTION

Over the next five years, at least five private companies around the world plan to launch commercial remote sensing satellites able to detect objects as small as one meter across. That level of detail is not as good as that of current government-controlled spy satellites, which by most accounts can achieve a resolution of just a few centimeters, but it is getting close. One key difference renders the commercial satellites far more interesting and possibly far more destabilizing than the state-owned spy satellites: the operators of these systems are not going to hide the imagery in the bowels of intelligence agencies, but are going to sell it to anyone able and willing to pay. The new commercial satellites will make it possible for the buyers of satellite imagery to, among other things, tell the difference between trucks and tanks, expose movements of large groups such as troops or refugees, and determine the probable location of natural resources.

Whether this increased access to imagery amounts to a positive or negative development depends on who chooses to use it and how. On the plus side, governments, international organizations, and nongovernmental groups may find it easier to respond quickly to sudden movements of refugees, document and publicize large-scale humanitarian atrocities, monitor environmental degradation, or manage international disputes before they escalate to full-scale interstate wars. The United Nations, for example, is looking into the possibility that satellite imagery could significantly help curtail drug trafficking and narcotics production over the next ten years. Similarly, the International Atomic Energy Agency is studying the utility of

commercial high-resolution satellite imagery for monitoring state compliance with international arms control agreements.

But there is no way to guarantee benevolent uses. Governments, corporations, and even small groups of individuals could use commercial satellite imagery to collect intelligence, conduct industrial espionage, plan terrorist attacks, or mount offensive military operations. Even when intentions are good, it can be remarkably difficult to derive accurate and useful information from the heaps of transmitted data. The media, for one, have already made major mistakes, misinterpreting images and misidentifying objects, including the number of reactors on fire during the Chernobyl nuclear accident in 1986 and the location of the Indian nuclear test sites just last year.

Such bloopers notwithstanding, the new satellite imagery will provide many people with information to which they never before had access. The implications for national sovereignty, international peace and security, the ability of corporations to keep proprietary information secret, and the balance of power among the former holders of information (a few industrialized states) and the newly informed (other governments and global civil society) are serious. Undoubtedly states will attempt to maintain tight controls over this new source of information. Whether their efforts will succeed remains to be seen.

In short, the new form of transparency brought about by the advent of high-resolution commercial satellites raises a host of pressing questions. Does it portend an age of peace and stability, or does it create vulnerabilities that will make the world more unstable and violent? What contributions can emerging remote-sensing technologies make to the fields of news reporting, humanitarian relief, environmental protection, and international security? What policies could the United States and other countries adopt to secure the benefits of growing international transparency while limiting its potential negative consequences?

The Technology of Remote Sensing

An analysis of the implications of the new satellites requires a basic understanding of what the various existing and future systems can see and do, what the jargon used in the remote sensing field means, and what types of sensors exist.

Perhaps the best-known concept is that of *spatial resolution*. Spatial resolution refers to the size of the objects on the ground that the satellite sensor is able to detect. A satellite image is a mosaic. A sensor applies one value (a shade of grey or color) to each square of the mosaic. For a satellite with 1-meter resolution, each square in the mosaic corresponds to one square meter of ground area, while 10-meter resolution corresponds to ten square meters on the ground—a difference of a factor of 100 (see image on page 26).

At present, civilian and commercial satellites carry one of three types of sensors: film, electro- optical, and synthetic aperture radar (SAR).

Film sensors take actual photographs, with the film returned to Earth either by retrieving ejected film capsules or by recovering the entire satellite. Both U.S. and Soviet spy satellites started off using film, and many Russian satellites still do. Film provides good high-resolution imagery but has two real drawbacks. It can be slow, since it usually has to be physically retrieved and developed, and the satellite becomes useless once it runs out of film, a characteristic that requires frequent launches of new satellites.

Electro-optical sensors overcome these disadvantages. They measure the electromagnetic radiation reflected off or emitted by objects on the Earth's surface, creating digital images of ground features that are then transmitted to receiving stations on Earth in a matter of minutes. However, these systems, like film, do not produce their own signals and therefore depend on other sources of energy such as the sun to illuminate the objects being observed. This characteristic constrains the use of both types of systems to daylight hours and favorable conditions. Bad weather or smoke can severely limit what these systems can see.

There are three different types of electro-optical sensors. Panchromatic sensors detect energy reflectance in only one band of the electromagnetic spectrum and thus produce black-and white imagery. Multispectral sensors can measure electromagnetic reflectance in several different color bands—usually three to seven—and so produce color images. Hyperspectral sensors, through a similar technique, image objects using many different spectral bands. The ability of hyperspectral sensors to distinguish tens and sometimes hundreds of different shades of color allows them to provide a great deal of information about the composition of features on the Earth's surface not discernible by either panchromatic or multispectral instruments.

With synthetic aperture radar sensors, the systems transmit a signal in the microwave part of the spectrum to the Earth's surface and then detect the characteristics of the return signal after it reflects off objects on the surface. Because radar satellites emit their own signals and operate in longer wavelengths than electro-optical systems, their operations are not limited to daylight hours. Synthetic aperture radar sensors can image any spot on Earth day or night, in any weather, through clouds and smoke. As with the electro-optical systems, they produce digital data that can be downloaded to ground receiving stations moments after the images are collected.

APPLICATIONS OF EMERGING REMOTE SENSING CAPABILITIES

In 1858 the French photographer Gaspard-Felix Tournachon (popularly known as Nadar) pioneered the field of remote sensing when he took the world's first aerial photograph of Paris from his gas balloon, Le Géant, 250 feet above the ground. Two years later Nadar found himself taking aerial pictures of enemy troop movements during the 1870 Franco- Prussian war.(2) What had started as one man's desire to capture the imagination of the world through the lens of a camera suddenly found novel applications in the bloody field of interstate warfare.

Since those early days, many more applications have been discovered for remote sensing data. Although the age of easy access to timely high-resolution satellite imagery is just now dawning, for several decades imagery has been available from aircraft and even (at lower resolutions) from government-operated satellites (see Chapter Three and Appendix B). Over the past thirty years, governments, corporations, and nongovernmental organizations have used aerial and space-based imagery platforms to, among other things, collect intelligence, execute military operations, plan development projects, and monitor the environment. It seems likely that as the availability of high-resolution imagery grows, and especially if the prices drop, governments and non-state actors will find new arenas where remote sensing data can be of value.

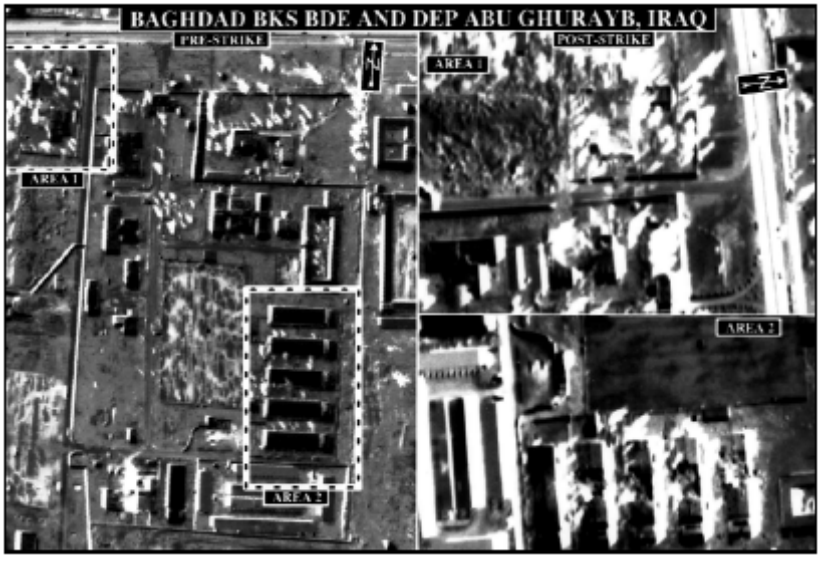
Although a discussion of the full range of applications for remote sensing data is beyond the scope of this monograph, the brief overview that follows provides a glimpse of the multifaceted significance of this powerful form of global transparency.

Security Applications

Of all the applications of commercial high-resolution satellite imagery, the most controversial and the most lucrative are its security applications.(3) In the short term, nearly half the sales of high-resolution imagery will be made to defense and intelligence organizations worldwide.

High-resolution commercial satellite imagery can help governments, especially those with no indigenous imagery collection capabilities, monitor the activities of neighbors and regional adversaries and expose violations of international norms and treaties. In August 1987, for example, the German foreign intelligence service, the Bundesnachrichten Dienst, used 10-meter resolution SPOT imagery to publicize the construction of a chemical warfare production facility near Rabta, Libya.(4) Space-based reconnaissance is particularly well suited for this type of intelligence collection because it is sanctioned under international law and is considerably less intrusive than either aerial or on-ground surveillance. An added advantage of commercial satellite imagery is that it can be shared. Whereas government officials closely guard spy satellite images to conceal the technical capabilities of national reconnaissance systems, commercial imagery can easily be shared with foreign governments and international organizations, a considerable advantage in multilateral operations such as those in Iraq, Bosnia, or Kosovo.

In addition to intelligence collection, high-resolution commercial satellite imagery can help identify enemy vulnerabilities, plan military operations, assess strike effectiveness, and prioritize targets for follow-up missions. There is some evidence that the Iraqi military may



Bomb damage assessment photos released by the U.S. Department of Defense on December 17, 1998, of the Baghdad Directorate of Military Intelligence Headquarters.

have used 10-meter resolution SPOT satellite photographs for attack planning and post-attack assessments both during the eight-year Iran-Iraq war and prior to the invasion of Kuwait in August 1990.(5) SPOT and Landsat imagery later helped the allied forces expel the Iraqi troops from Kuwait.(6)

Technological advances are likely to increase the demand for commercial satellite imagery. With the launch of the world's first hyperspectral sensors on board the OrbView 4, Naval

EarthMap Observer, and Aries satellites, all of which are scheduled to begin operations within the next three years, security agencies worldwide will have access to richer data for intelligence gathering and military planning. Hyperspectral imagery can detect any type of camouflage that is not natural and growing. Green plastic and foliage have unique spectral signatures that are easily distinguishable from living vegetation. Military planners can use such information to design and carry out precision strikes against concealed high-value targets. In addition, hyperspectral sensors may be able to identify high concentrations of different chemicals in the soil.(7) It may be possible to employ these sensors to monitor, document, and publicize the production and use of chemical weapons in different parts of the world.

There is no reason to believe that the demand for commercial satellite imagery for intelligence collection and military planning will abate any time in the near future. As long as armed conflicts occur, government demand for remote sensing data is likely to remain high, regardless of what happens to the prices of satellite imagery. If anything, with the launch of new systems with better spatial and spectral resolutions and shorter turnaround times, demand will continue to grow.

Humanitarian Application

On August 10, 1995, Madeleine K. Albright, at the time the United States' chief delegate to the United Nations, called the attention of the international community to atrocities committed by Bosnian Serbs against Bosnian Muslims after the fall of the UN "safe area" in Srebrenica.(8) Amb. Albright presented the UN Security Council with American spy satellite images that showed people herded into a soccer field at Nova Kasaba the previous July 13 and 14. Imagery collected several days later revealed an empty stadium but mounds of freshly dug earth in the nearby field. After the end of hostilities, war crimes investigators exhumed the graves and recovered the bodies of dozens of Bosnian Muslims(9).

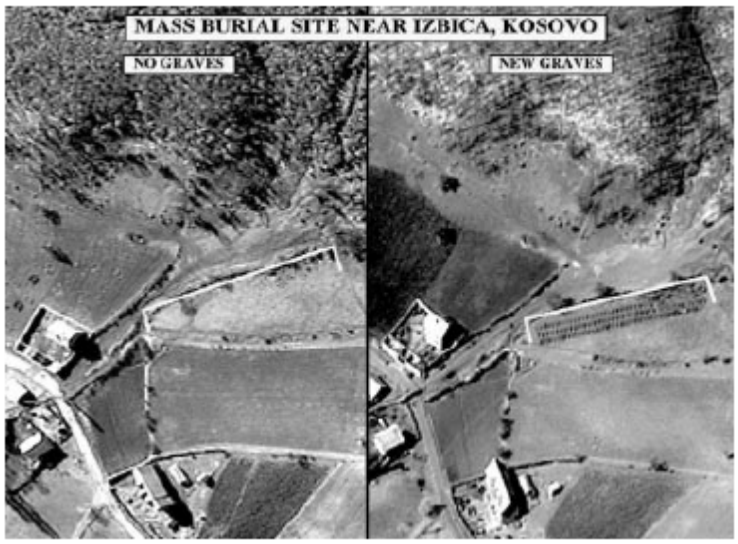
The 1995 incident unveiled to the world the power of satellite imagery in monitoring, documenting, and, possibly, deterring large-scale humanitarian crises. On April 1, 1999, as a new chapter of Serbian aggression was being written, this time against Kosovar Albanians, members of ten human rights and religious organizations gathered at the National Press Club in Washington, D.C., to call upon the Clinton administration to "immediately provide the International Criminal Tribunal for the Former Yugoslavia with all available intelligence information that reveals evidence of atrocities in Kosovo, specifically imagery collected by satellites, aircraft, and unmanned air vehicles."(10) Responding to such demands, the United States and the North Atlantic Treaty Organization (NATO) released numerous satellite images of mass graves in different parts of Kosovo, including Glodane, Velika Krusa, Pusto Selo, Glogovac, and Izbica.

The flood of spy satellite imagery made available to the public during the Kosovo crisis was unprecedented. It is not clear, however, whether the United States and its NATO allies will be so open again. Publicizing the egregious acts of the Serbian forces in Kosovo clearly served the political objectives of the Clinton administration, which was trying to win the support of the international community in general and the American public in particular. It seems doubtful that a future U.S. administration would be as forthcoming if releasing spy satellite imagery meant having to take action against states with close ties to the United States or having to consider undertaking a major engagement in less strategically significant parts of the world, such as Rwanda, Sudan, or Afghanistan.

The advent of commercial high-resolution satellites will guarantee that in the future the Milosovics of the world will not be able to carry out their sinister plans unobserved. Satellites can document events in the remotest corners of the world, or in areas where security concerns limit access to international observers and media groups. Such information can later be used to publicize humanitarian emergencies and possibly punish the perpetrators of humanitarian crimes. Commercial satellite operators are generally not restrained by the sort of political constraints that often muzzle the response of state governments. Whereas states may refrain from publicizing acts of humanitarian violence in other friendly countries or in countries where they do not wish to get involved, commercial satellite operators will readily market such imagery to a host of media and human rights groups. Such widely available satellite imagery might deter states from committing large-scale violence against ethnic minorities and might compel the international community to take action once such acts of violence are committed.



United States surveillance photograph in a handout presented by the chief U.S. delegate to the United Nations on August 10, 1995, showing alleged mass graves in Nova Kasaba, Bosnia (later found to contain bodies of Muslim civilians massacred by the Bosnian Serbs).



Aerial imagery from a NATO handout released on April 17, 1999, showing what NATO described as new graves near Izbica, Kosovo.

High-resolution satellite imagery can also provide state and non-state actors with valuable information on how to respond to humanitarian emergencies. Large refugee movements can be tracked using imagery with a resolution of 1 meter or better. Such imagery could help determine the direction of refugee flows, the size of different refugee pockets, ground surface

features, and the resources available to humanitarian response teams. Employing high-resolution satellite imagery to plan relief operations could significantly improve the ability of various groups to alleviate human suffering in the wake of large-scale humanitarian emergencies.

Environmental Applications

For the past twenty-seven years, low and medium-resolution civilian satellites have provided invaluable data on the status of the Earth's temperature, land cover, water bodies, and atmosphere.(11) For example, satellite imagery has allowed scientists to monitor and document the depletion of the ozone layer over the South Pole, the shrinking of the Aral Sea



Five-meter-resolution imagery taken by the Indian Remote Sensing satellite (IRS-1D) on May 8, 1999, depicting the destruction left behind in the wake of a powerful tornado near Oklahoma City.

in the former Soviet Union, and the rate of loss of the tropical rainforests in the Amazon basin. In addition, remote sensing systems have at times played a central role in managing serious environmental emergencies. After the 1990-1991 Persian Gulf War, the thermal-infrared sensors on board the Landsat 4 satellite provided firefighters with critical information on the exact location of some 529 oil fires in liberated Kuwait.(12) More recently, the Canadian RADARSAT-1 system helped avert a potential disaster by providing timely information on the size and direction of a large oil slick near the water intake pipes of a nuclear power plant on the coast of Japan.

As these examples illustrate, remote sensing systems have for decades satisfied many of the data needs of various government agencies, scientists, and environmentalists. In the future, emerging commercial satellites with higher spatial and better spectral resolutions will supplement and complement (but not replace) existing environmental monitoring capabilities. The primary reason is that most environmental changes are slow, evolving processes that take place across extensive tracts of Earth over lengthy periods. To monitor and document long-term environmental change, scientists need continuous coverage of vast regions. The existing high price of commercial satellite imagery makes it virtually impossible for anyone except the most affluent environmental organizations to purchase large quantities of high-resolution satellite imagery. Whereas the U.S. government provides Landsat 7 pictures for $475 to $600 per scene, commercial satellite operators routinely charge $4,400 for a comparable product. Although these prices may decline as the number of commercial systems in operation increases, that drop is unlikely any time soon, given that the commercial satellite companies are trying to recoup investments on the order of hundreds of millions of dollars.

While existing civilian satellites have a comparative advantage in long-term, wide-area monitoring of the environment, emerging commercial satellites seem to be particularly well suited for periodic assessments of areas of greatest concern. Possible environmental applications of emerging commercial satellites include: studying the impact of land development and energy exploration on wilderness areas, developing more complete wetland inventories, monitoring the health of vegetation in all regions of the world but particularly in remote or inaccessible areas, and detecting toxic discharges from mines and production facilities.

Governments, corporations, and conservation groups are slowly beginning to understand the immense potential of remote sensing data for environmental monitoring and are taking steps to better incorporate such data into their decision making. In 1995 the U.S. Environmental Protection Agency (EPA) conducted a study on the possibility of employing hyperspectral sensors to monitor toxic runoffs from abandoned mines. It conducted the experiment at the CalGulch Mine Superfund site in Leadville, Colorado, which is home to hundreds of relict gold, silver, lead, and zinc mines suspected of contributing acid drainage and heavy metals to downstream supplies of drinking water. Using NASA's aerial hyperspectral sensor, the Airborne Visible and Infra-Red Imaging Spectrometer (AVIRIS), the EPA was able to study the site while saving approximately "80 percent of the time and cost of traditional ground-based analysis."(13) After the success of the CalGulch Mine experiment, the EPA launched an Advanced Measurement Initiative (AMI) to accelerate the adoption and application of remote sensing and other technologies that could provide more timely, accurate, and cost-effective environmental monitoring data. Under the initiative, the EPA has undertaken two new projects involving hyperspectral sensors to monitor the presence of jarosite (a mineral that can contribute to acid drainage and the release of heavy metals into the environment) in the Ray copper mines in Arizona, and to measure the concentration of suspended minerals, chlorophyll, and dissolved organic carbon in the surface waters of the Neuse River in North Carolina. The results of both studies were to be released at the end of 1999.

Mindful of the bad publicity associated with lax environmental practices, a number of multinational corporations have also begun using remote sensing technologies to police their own activities. The Texas oil giant, Texaco, for example, developed an aerial hyperspectral sensor called Texaco Energy and Environmental Multispectral Imaging Spectrometer (TEEMS) to help it pursue environmentally sound policies. Once fully operational, this imaging capability will allow Texaco to, among other things, establish environmental baselines prior to commencing exploration, conduct fracture analysis on its vast network of pipelines, identify oil seeps and oil spills, and, when necessary, take action to minimize and reverse damage done to the environment.

The use of remote sensing data for environmental monitoring is not limited to state governments and large corporations. Environmental nongovernmental organizations have for years made extensive use of existing relatively low-resolution imagery to monitor enforcement of the U.S. Endangered Species Act, document the destruction of coral reefs around the world, and generate plans for ecosystem management.(14) As more sophisticated commercial remote sensing systems become available, and especially if the prices drop, it can be expected that environmental groups will expand their activities, monitoring compliance with existing environmental standards and publicizing violations.

Media Uses of Satellite Imagery

On Saturday, April 26, 1986, two explosions destroyed Unit 4 of the Chernobyl nuclear power plant in Ukraine and released 100 million curies of radionuclides into the environment.(15) Hoping to keep the incident secret, the Soviet government immediately sealed off a 100- mile radius around the stricken reactor and banned all foreign travel to Kiev, the largest city nearest the site of the accident.(16) Two days later, as radioactive clouds began setting off radiation alarms throughout Europe, the Soviet news agency Tass confirmed Western suspicions by disclosing that one of its atomic reactors had indeed been damaged.

Within hours of the announcement the United States' top-secret spy satellite, Keyhole (KH-11), began collecting imagery of the Chernobyl power station. By Tuesday, April 29, KH-11 photos were in the hands of U.S. policy makers in Washington, D.C. But this time government officials did not have exclusive access to satellite imagery. Less than twenty-four hours after Keyhole images reached the White House, the American Broadcasting Company (ABC) aired medium-resolution Landsat images of the blazing nuclear reactor.(17) Shortly thereafter, a number of media organizations began broadcasting higher resolution SPOT images of the Chernobyl power plant.

In the decade and a half since the Chernobyl accident, the use of satellite photos by news organizations has increased significantly. Despite the relatively low resolution of publicly available satellite systems, media groups have employed remote sensing technology to report on important events such as the military buildup in the former Soviet Union, the Persian Gulf War, weapons proliferation in the third world, the U.S. assault on Osama bin Laden's hideaway in Afghanistan, the devastation left by a tornado that swept through Oklahoma City, the nuclear tests in India and Pakistan, and, more recently, the humanitarian atrocities in Kosovo.

With the advent of commercial high-resolution satellites, the use of remote sensing imagery by media groups is likely to grow. Imagery, even relatively fuzzy commercial satellite photos, allows news agencies to convey important information visually to their audiences. More important, satellites can go places that are otherwise inaccessible to media groups. These two features alone will ensure the continued use of satellite imagery by news organizations for years to come.

Business Applications

The full range of commercial applications for satellite imagery is not yet known. A number of factors, including cost, timeliness, and spectral as well as spatial resolution, will ultimately determine how narrowly or broadly remote sensing imagery is employed. However, several commercial applications of satellite imagery are worth noting here.

Satellite imagery has important applications in map making. While 95 percent of the world's land mass is mapped at a scale of 1:250,000, only 33 percent is mapped at 1:25,000. Less than 10 percent of Africa and South America and less than 20 percent of Asia and Australia are mapped at the higher scale. In many cases the maps available at the higher scale are outdated or incomplete. Emerging high-resolution commercial satellites will significantly improve both the scale and quality of maps of the more remote and less developed regions of the world.

Another major commercial application of high-resolution satellite imagery is in the field of agricultural management. Agriculture is a volatile field with pronounced effects on the economic well-being and political stability of nations. Satellite imagery can help take some of the unpredictability out of this important sector. Multispectral and hyperspectral sensors are well suited to predicting crop yields, detecting crop disease and insect infestation, and monitoring thermal stress.(18) Satellite imagery can be used to prepare detailed maps of agricultural fields to determine the best seeding and irrigation patterns, as well as the optimum amounts of fertilizer and pesticides needed to obtain higher crop yields.

Satellite imagery can also help pinpoint the probable location of nonrenewable natural resources, a capability that can dramatically reduce the economic risks of exploration. Radar imagery, for example, has for years helped oil companies identify new offshore oil reserves. According to Roger Mitchell of the Earth Satellite Corporation, nearly 80 percent of offshore oil exploration starts by searching for oil seeps.(19) Oil's viscosity retards wave formation, causing a "calm spot" on the ocean surface. Radar satellites can detect these calm spots and analyze their suitability for future exploration.

Similarly, hyperspectral sensors can inspect the Earth's surface for unique spectral signatures associated with particular resources. Once a signature is detected, mining companies can begin exploration activities with much greater confidence. In the next few years, hyperspectral sensors may revolutionize exploration for natural resources in all corners of the world. Unlike the traditional methods, satellites can image any region on Earth regardless of its accessibility and can provide accurate information at a significantly lower cost. However, for hyperspectral imagery to be useful, additional research is needed to compile a more thorough library of the spectral signatures associated with different natural resources.

Urban planners can also use satellite imagery to improve efficiency and reduce costs. Houses, water tanks, canals, sidewalks, pavements, and parking lots are easily distinguishable on high-resolution satellite imagery. City officials can use such information to plan new development projects and design improved networks of public utilities. Remote sensing data can provide engineers and construction companies with valuable information on soil composition and structural morphology before substantial investments are made.

Finally, remote sensing data provide corporations new opportunities to spy on their competitors. A comparison of archived and more recent satellite imagery can reveal important information about the production capacity of rival companies at dispersed locations around the world. For example, high-resolution satellite imagery can reveal new construction, new types of shipping containers on loading docks, or an increase in the number of rail cars used to distribute products.(20) Although traditionally observers on the ground have obtained such information, commercial satellite imagery may prove to be more cost-effective and significantly less intrusive.

Competitive Intelligence or Industrial Espionage?

There has never been a ruling on the legality of space-based imagery for competitive intelligence. The only relevant case, which may form the basis for all future litigation, dates back to 1970. In *E.I. du Pont de Nemours & Co., Inc. v. Christopher*, DuPont sued the Christopher brothers for taking aerial pictures of its Texas plant while the plant was under construction to learn DuPont's new process for methanol production (Fred Wergeles, "Commercial Satellite Imagery: New Opportunities for Competitive Intelligence,"

Competitive Intelligence Magazine). In this case, the court ruled in DuPont's favor, citing the steps taken by the company to protect its trade secrets and the improper means used by the Christopher brothers to uncover those secrets.

The advent of commercial high-resolution satellite imagery may have a profound impact on how cases involving remote sensing imagery are adjudicated in the future. In *DuPont* the court adjudged the actions of the Christophers to be improper primarily because, at that time, the method they used to determine DuPont's secrets was considered so out of the ordinary (Fred Wergeles, "Commercial Satellite Imagery: New Opportunities for Competitive Intelligence," *Competitive Intelligence Magazine)*. Once high-resolution satellite imagery becomes widely available, it will be harder to argue that overhead observation of the production facilities of rivals is an extraordinary and, therefore, improper means for carrying out competitive intelligence. Instead, businesses may have to take additional steps to protect valuable trade secrets.

Even assuming that the use of satellite imagery for competitive intelligence is considered unlawful, it will be difficult for corporations to prove any wrongdoing by industrial competitors. Current statutes do not require satellite operators to disclose either their imagery or the identity of their clients to third parties. Thus, it is nearly impossible for companies to know whether a passing satellite collected imagery of their facilities and, if so, who asked for specific images. This task becomes even more arduous as the number of domestic and, more importantly, international sources of high-resolution imagery increases. Whereas greater regulation and closer government scrutiny can restrain domestic vendors, controlling international vendors is likely to prove far more elusive.

DRAWBACKS OF COMMERCIAL SATELLITE IMAGING

The widespread availability of commercial high-resolution satellite imagery will for the first time reveal to many people and organizations information to which they never before had access. Some have celebrated this new development, calling it the emerging era of global transparency. But transparency has both positive and negative consequences.

In the field of international relations, greater transparency could allay tensions among international rivals and herald a new era of peaceful coexistence. As one observer stated, "Nations that know what their enemies are doing are less likely to increase world tensions through activities born of fear. And nations that know their enemies are observing them are far less likely to threaten international peace through rash behavior."(21) According to this view, if everyone is constantly watching everyone else, surprise attacks become impossible and aggressive actions unrewarding.

This premise may often be true, but not always. When the success of aggression is dependent on the element of surprise, transparency will indeed reduce the incidence of aggression. But not all aggression requires surprise to succeed. Transparency could aggravate interstate conflicts by removing ambiguities about relative capabilities and allowing states to exploit each others' weaknesses. To the degree that governments new to remote sensing misinterpret what they see, imagery could create groundless fears.

Even under the best of circumstances, transparency cannot ensure that the right decisions are made. Transparency reveals behavior, but not intent.(22) If enemy troops are detected

massing along the border, is that just harmless posturing, or are they preparing for a preemptive strike? If states reach the wrong conclusions, they may find themselves spiraling uncontrollably toward war.

Transparency could also complicate decision-making by introducing new participants into the policy process. Widespread availability of high-resolution satellite imagery would allow private citizens, nongovernmental organizations, and particularly the media to take a more active role in policy making. These groups could independently use satellite imagery to monitor state compliance with international agreements, expose environmental degradation, and publicize large-scale humanitarian emergencies. In some situations civil society groups and the media might be able to compel states to take action, even when government officials would much prefer to do nothing.

Here again, there are no guarantees that greater transparency will produce better outcomes. Nongovernmental organizations and the media rarely have the resources, analytical skills, or technical expertise that are more readily available to state governments. It is inevitable that organizations will make mistakes as they begin to increasingly rely on satellite imagery. The media have already made such errors on at least four occasions. During the 1986 Chernobyl accident, in an attempt to be the first with breaking news, a number of media organizations misinterpreted imagery and erroneously reported that two nuclear reactors had melted down.(23) Just a few weeks later, a number of networks in the United States cited SPOT imagery of a Soviet nuclear proving grounds at Semipalatinsk as evidence of Moscow's decision to resume nuclear testing. Further analysis revealed that the networks had completely misinterpreted the imagery, falsely presenting routine activities in a far more pernicious light.(24)

Another error occurred in 1992 when a newspaper called the *European* published SPOT images of what it labeled an Algerian nuclear research complex. Subsequent analysis of the image revealed that the feature in the photo was not a nuclear research facility but a military airbase. To make matters worse, the *European* had published the image upside down and backwards.(25)

More recently, on May 25, 1998, *Newsweek* magazine published a satellite image that it claimed showed the site in the northern desert state of Rajasthan where India had conducted five nuclear tests. *Newsweek* maintained that the image dated from a week before the tests and ran the picture with several captions identifying specific objects and installations. None of the information was correct. It turned out that the imagery had been collected over five years prior to the blasts, and the feature *Newsweek* identified as the hole where one of India's nuclear explosions took place was in fact an animal holding pen.(26)

Fortunately, no grave damage has yet resulted from the erroneous reports that have appeared, but it is optimistic to think that continued carelessness will have no consequences. False reporting, whether deliberate or unintentional, could easily embitter relations among nations and prevent the resolution of outstanding disputes.

Transparency raises major economic concerns as well. Radar, multispectral, and especially hyperspectral sensors may allow extraction companies to know more about a country's natural resources than the country's own government. This disparity in knowledge could place state officials at a considerable disadvantage when negotiating drilling rights and mining agreements. As mentioned, governments are not the only ones that may feel an acute

sense of vulnerability. Corporations may find themselves being observed by competitors trying to keep tabs on their construction of new production facilities around the world and estimate the size of their production runs by looking at their emissions.

In short, the emerging global transparency resulting from high-resolution commercial remote sensing satellites promises both benefits and costs. The challenge is to devise policies that harness the benefits of growing international transparency while minimizing its many potential negative consequences.

CONCLUSION

This telephone has too many shortcomings to be seriously considered as a means of communication. The device is inherently of no value to us.
—Western Union internal memo, 1876

Heavier-than-air flying machines are impossible.
—Lord Kelvin, president, Royal Society, 1895

The wireless music box has no imaginable commercial value. Who would pay for a message sent to nobody in particular?
—David Sarnoff's associates in response to his urgings for investment in the radio in the 1920s

I think there is a world market for maybe five computers.
—Thomas Watson, chairman, International Business Machines (IBM), 1943

There is no reason anyone would want a computer in their home.
—Ken Olson, president and founder, Digital Equipment Corporation, 1977

640K ought to be enough for anybody.
—Bill Gates, Microsoft Corporation, 1981

The success rate of prognostications about how new technologies will fare approaches zero. No one really knows whether a thriving satellite commercial remote sensing industry will develop over the next decade, or whether the whole industry will crash, figuratively if not literally.

The only sure prediction is that the industry will change, drastically, in the next few years. Some of those changes may come in the form of technological improvements. Space Imaging, operator of the IKONOS satellite now in orbit, recently announced that it is thinking about follow-ons with even greater capabilities. Chief Executive Officer John Copple noted in an interview that the market has changed notably in the four years since the company was formed. Not only is there competition from other potential satellite operators, but "we're seeing much higher resolution from the aerial companies and would like to be able to participate in that market."(27) Although there is a widespread myth that Presidential Decision Directive-23 limits the resolution of American satellites to no better than 1 meter, in fact there is no constraint on resolution. Indeed, under ideal conditions IKONOS and some of the other satellites scheduled for launch within the next year will achieve resolutions closer to

0.86 meter. Copple says that the U.S. national security industry, likely to be a major customer, is urging U.S. companies to move to higher resolutions in future satellites.(28)

Some of the changes may involve the organization of the industry. Spot Image of France and OrbImage of the United States recently announced plans for a partnership that would market OrbImage's high-resolution imagery (from OrbView 3 and OrbView 4, planned for launch in late 2000) through Spot's well-established global sales network.(29) Such cross-border alliances are becoming emblematic of the globalization of the industry. Not only are there many countries with civilian or commercial operators, the operators themselves are increasingly multinational enterprises.

If commercial satellite remote sensing does take off, the new availability of imagery will raise further questions for government officials and others around the world, questions not easily answered through purely national means. Because information really is power, the spread of this particularly vivid and comprehensive form of information will ripple through all sorts of relationships—those among states, and those between states and other international actors such as businesses and civil society.

The rapidly growing literature and plethora of conferences on the new satellites have mostly focused on what the availability of high-resolution imagery will do to the conduct of war, and in particular whether it will undermine the overwhelming military preponderance of the United States. Certainly it is possible to imagine circumstances in which the United States would benefit militarily from the suppression of such imagery. It is more difficult to imagine military conflicts involving the United States in which France, India, Israel, Russia, and eventually China would all agree to go along with the suppression of such imagery. This battle is already lost.

The more fundamental questions raised by the new satellites have to do with basic issues about the meaning and relevance of national borders, about the relationships of governments not only to one another but also to private businesses and nongovernmental organizations, and about the meaning of national sovereignty. Satellite imagery is only one of a whole series of information technologies that have caused states to lose control over information about what is happening within their borders. From now on, it will not only be the U.S. Ambassador to the United Nations who can show images of atrocities in the UN Security Council and demand action. Any government on the council will be able to do so, or any government or nongovernmental organization that can persuade a council member to present the images. International negotiations on everything from arms control to climate change, already populated by ever-growing numbers of governments, businesses, and nongovernmental organizations, will face new complications caused by their inability to suppress or ignore unwanted information. Because information will be so widely available, crises may become harder to manage, as leaders find themselves under relentless pressure to act quickly.

But this is not the first time the world has had to adjust to a technologically driven jump in the availability of information. Printing presses were once seen as tools of the devil because they removed control over information from the hands of the medieval Catholic Church and spread it across the (literate) populace at large. Every new step from the telegraph to the Internet has been greeted with proclamations of apocalyptic change. Governments that have tried to suppress and control flows of information have, in the long run, suffered for it. The

wiser course of action, as well as the only practicable one, is to learn to live with the new transparency.

For the United States in particular, it is most unlikely that the shortsighted policy of shutter control will do good, and it could do harm even to the United States itself by undermining an industry on which the national security community will increasingly have to rely. The United States would be better served by policies that return to the traditional U.S. emphasis on open skies and freedom of information. In the 1960s, U.S. policies helped bring about the legitimacy of satellite reconnaissance. In the 1970s and 1980s, U.S. leadership in both the technology and politics of civilian remote sensing led to global acceptance of unconstrained imaging from space. When the inevitable international disputes arise over the new transparency, and when the United States finds itself facing short-term interests in suppressing imagery, it is crucial that it stick to the long-range policies in favor of transparency that have served it so well.

For the rest of the world, this new form of transparency will do far more good than harm. Countries that now live in fear of one another will be able to learn whether those potentially hostile neighbors are in fact mobilizing for attack, and would-be attackers, at least sometimes, will be deterred by the overwhelming likelihood of detection. The pressing environmental and developmental problems facing poor countries, heretofore unseen and therefore easily ignored by the rich, will become both more visible and better understood.

Most important, the new imagery will contribute to a badly needed shift in perspective. As Oliver Morton wrote in an article on satellite imagery in *Wired* magazine in 1997:

> Like the telephone or the wrist watch, it is the sort of product that gets woven into the fabric of life—in this case, as an assumption that all the world is out there to be seen, that it is all available, comprehensible, and held in common…. With shared eyes we will watch the world carry its cargo of civilization —its roads, its fields, its cities, its landfills—through time and space. This portrait will be an image that can zoom in to the personal and pull out to the geopolitical, a new way to look at borders, a new way to look at news. It will be an illustration of everything: not, in the end, a view from nowhere, but a view from everywhere, for everyone.(30)

NOTES:

1. For the Real Video, transcripts, and summary of different presentations at the conference, visit the Carnegie Endowment for International Peace website at www.ceip.org/programs/transparency/RemoteSensingConf/Agenda.htm.
2. Ralph Rugoff, "Fame," *LA Weekly*, July 30, 1999.
3. For a discussion of the security implications of commercial high-resolution satellites, visit the Carnegie Endowment for International Peace website at www.ceip.org/programs/transparency/RemoteSensingConf/BakerPage.htm; www.ceip.org/programs/transparency/RemoteSensingConf/BernsteinPage.htm; and www.ceip.org/programs/transparency/RemoteSensingConf/MullenPage.htm.
4. Peter D. Zimmerman, "The Uses of SPOT for Intelligence Collection: A Quantitative Assessment," in Michael Krepon, Peter D. Zimmerman, Leonard S. Spector, and Mary Umberger, eds., *Commercial Observation Satellites and International Security* (Washington, D.C.: Carnegie Endowment for International Peace, 1990), p. 77.
5. It is well documented that during the Iran-Iraq war, images of battle areas were purchased frequently. It is not clear, however, who acquired the imagery or for what purposes. See Peter D. Zimmerman, "From the SPOT Files: Evidence of Spying," *Bulletin of the Atomic Scientists*, Vol. 45, No. 7 (September 1989), p. 24. Further, it has been reported that "before invading Kuwait, Saddam Hussein bought imagery from the French SPOT

satellites," although the information could not be corroborated by the authors. See also Robert Wright, "Private Eyes," *New York Times Magazine*, September 5, 1999.
6. Report 102-539, U.S. House of Representatives, Committee on Science, Space, and Technology, May 28, 1992, p. 26.
7. This level of detail is possible only if the sensor has a high enough spatial resolution and can detect objects in the long-wave segment of the spectrum.
8. For more details visit the Carnegie Endowment for International Peace website at www.ceip.org/programs/transparency/RemoteSensingConf/PikePageHumanitarian.htm.
9. David Rohde, "A High-Tech Threat with a Low-Tech Track Record,"*New York Times*,April 4, 1999, p. 6.
10. The groups included: Physicians for Human Rights, Refugees International, International Crisis Group, Network Bosnia, Coalition for International Justice, Institute for the Study of Genocide, Freedom House, Network of East-West Women, Balkan Action Council, and Minnesota Advocates for Human Rights. Nora Boustany, "The Heavens Look Down on Kosovo," *The Washington Post*, April 2, 1999, p. A19.
11. For more details, visit the Carnegie Endowment for International Peace website at www. ceip.org/programs/transparency/RemoteSensingConf/HammondPage.htm and www.ceip.org/programs/transparency/RemoteSensingConf/JanetosPage.htm.
12. The retreating Iraqi troops set between 640 and 650 oil wells alight; some, however, were already extinguished by the time Landsat imagery of the oil fields was collected. Peter D. Zimmerman, "The Use of Civil Remote Sensing Satellites During and After the 1990-91 Gulf War," *Verification Report*, VERTIC (1992), p. 239.
13. Frederick P. Hafetz and Gwen M. Schoenfeld, "Advanced Measurement Techniques: Technological Breakthroughs May Usher in Era of Change," *Environmental Compliance & Litigation Strategy*, Vol. 13, No. 3 (August 1997), p. 1.
14. Karen Litfin, "Public Eyes: Satellite Imagery, the Globalization of Transparency, and New Networks of Surveillance," unpublished manuscript, 1999.
15. For more details on the media uses of satellite imagery, visit the Carnegie Endowment for International Peace website at www.ceip.org/programs/transparency/RemoteSensingConf/DubnoPage.htm and www.ceip.org/programs/transparency/RemoteSensingConf/LivingstonPage.htm.
16. Oliver Morton, "Private Spy," *Wired* (August 1997), p. 1.
17. Ibid., pp. 9-10.
18. Pierre C. Robert, "Remote Sensing: A Potentially Powerful Technique for Precision Agriculture," paper presented at the conference titled Land Satellite Information in the Next Decade II: Sources and Applications, American Society for Photogrammetry and Remote Sensing, Washington, D.C., 1997.
19. "Offshore Oil Detection: Radar Imagery Offers a Slick for Locating Rich Reserves at Sea," *Imaging Notes*, Vol. 14, No. 2 (March/April 1999), p. 24.
20. Fred Wergeles, "Commercial Satellite Imagery: New Opportunities for Competitive Intelligence," *Competitive Intelligence Magazine*, Vol. 1, No. 1 (April/June 1998), p. 37.
21. R. Jeffrey Smith, "High-Tech Vigilance," *Science* (December 1985), pp. 26-33.
22. Ann M. Florini, "The End of Secrecy," *Foreign Policy*, No. 11 (Summer 1998), p. 60.
23. Dino A. Brugioni, "Satellite Images on TV: The Camera Can Lie," *The Washington Post*, December 14, 1986, p. H1.
24. Ibid.
25. Vipin Gupta, statement made during the Carnegie Endowment for International Peace conference entitled No More Secrets: Policy Implications of Commercial Remote Sensing Satellite, Washington, D.C., May 26, 1999. To watch the Real Video of Vipin Gupta's presentation, visit the Carnegie Endowment for International Peace website at www.ceip.org/programs/transparency/RemoteSensingConf/GuptaPage.htm.
26. Statement made by Steven Livingston at the Carnegie Endowment for International Peace conference entitled No More Secrets: Policy Implications of Commercial Remote Sensing Satellites, Washington, D.C., May 26, 1999. See also "Correction" in the August 31, 1998 issue of *Newsweek*. To see more of Steven Livingston's presentation, visit the Carnegie Endowment for International Peace website at www.ceip.org/programs/transparency/RemoteSensingConf/LivingstonPage.htm.
27. Warren Ferster, "After IKONOS, Space Imaging Plans Even Better Satellite," *Space News*, Vol. 10, No. 36 (September 27, 1999), p. 3.
28. Ibid.
29. Warren Ferster and Peter B. de Selding, "Spot Image, Orbital Plan Reciprocal Sales Deal," *Space News*, Vol. 10, No. 36 (September 27, 1999), p. 3.
30. Oliver Morton, "Private Spy," *Wired* (August 1997), p. 9. FINALreport.qxd 2/17/00 6:54 PM Page 37

INTERNATIONAL VIEWS OF OSINT

TEACHING THE GIANT TO DANCE: CONTRADICTIONS AND OPPORTUNITIES IN OPEN SOURCE WITHIN THE INTELLIGENCE COMMUNITY

Admiral William Studeman

FAS Intro: The following discussion of the history of the Foreign Broadcast Information Service and open source intelligence was presented by Admiral William Studeman at the First International Symposium on Open Source Solutions in December 1992. It is reproduced here with the permission of Open Source Solutions, Inc.

It's a pleasure to be here today to take part in this symposium. This is truly an exciting time -- a revolutionary time -- to be in the intelligence business. And no area is full of more promise for intelligence than open source access and exploitation. In my only reference to dancing, you can consider this presentation as an attempt to describe how we move the Intelligence Community giant from the square dancing era of yesterday to the open source Lambada of tomorrow.

A number of people that I've talked to -- including Members of Congress, journalists, and the public -- have asked me to explain why intelligence organizations are interested in unclassified information. So I'd like to begin by asking a rhetorical question: "why does the Intelligence Community collect and analyze open source data?"

This in not a new issue for intelligence. As you know, intelligence has drawn broadly on open sources for many years. FBIS -- the Foreign Broadcast Information Service -- has collected, analyzed and reported open source intelligence from all over the globe for over half a century -- and it has done a superb and highly valued job.

The information that FBIS has collected over the years has been critical to US national security decision makers.

- Few people realize that during the 1962 Cuban missile Crisis, through monitoring Radio Moscow, FBIS provided President Kennedy with the first news of the Soviet decision to withdraw missiles from Cuba.
- At times, public information has been the Community's only source during a crisis. For example, during the 1956 Hungarian uprising and the 1968 invasion of Czechoslovakia, radio broadcasts provided intelligence analysts with highly relevant, timely understanding of what was happening in the streets of Budapest and Prague.
- Open sources can also provide tip-off or early warning of events. You may be interested to know that the change in policy leading to the February 1989 Soviet military withdrawal from Afghanistan was identified in FBIS media analysis reports as early as May 1985.
- More recently, CIA analysts who monitored the collapse of the Soviet Union estimate that at least 80% of their information came from open sources.

- And now, intelligence analysts are using open sources to monitor the Yugoslav crisis. They study transcripts of radio broadcasts by both sides to gain insights into the intensity of the conflict and the probable outcome.

Although all of the intelligence Community has relied on open sources for many years, some people who are not familiar with our business are confused about how intelligence uses information that is available to the public.

The first thing that people must understand is that intelligence is not competing with the media. But intelligence and the media are in the same business; that is, ultimately, to tell a story of relevant interest, but in our case, the story normally relates to a threat or a foreign issue of high or potential interest to U.S. or allied policymakers, planners, or warfighters. Our goal is not necessarily to produce raw open source data, but to glean information from open sources that is of interest to intelligence *as background* reference material for collectors and analysts/producers, and, more importantly as a source of information to be fused with data from classified sources and methods and this is again principally for the government customer.

Our analysts rely on a multiplicity of sources -- including signals, imagery, human and other classified intelligence sources as well as openly available data -- to produce their reports.

Foreign intelligence and counterintelligence earns its money first by maximizing these *classified* sources and methods, and secondly by building highly structured analysis and production systems which are highly responsive to the widest range of U.S. and allied customers, be the topic political, military, economic, environmental, sociological, law enforcement support, or otherwise.

But good intelligence officers, like media personnel, are essentially information hounds. The highest emphasis is placed on timeliness, relevancy, accuracy, and completeness of data disseminated at the lowest and most readily usable classification level and tailored to the diverse sets of simultaneous users at varying echelons of the bureaucratic structure from the President to lowest platoon leader and beyond.

The highest form of intelligence enlightenment is the dynamic and continuous fusion of data from all available sources. In this blending process a great synergy results, and this magic cannot be accomplished without unconstrained and continuous access to open source data. Open source can provide event specifics, background context, focus, contrast, improved accuracy, alarms, and many other positive features associated with data manipulation in an information age.

While untrustworthy data can often be associated with classified sources and methods, open source data can be a frequent source of biased and misleading information, or worse yet, the product of deliberate deception or information control practiced in parts of the world by a less free press that may also operate as a propaganda instrument of government forces. This dictates that a strong data evaluation system be in place for use with open source data, as it is for classified data.

On the positive side, when an open source contradicts other intelligence sources -- or other open source reporting -- it serves as a flag for the analyst to re-evaluate his or her analysis. For example, at a time when there was wide intelligence speculation that the Dominican

Republic might extradite a terrorist, an FBIS report called attention to a press account that the Dominican president had said he would not extradite the terrorist.

Utilizing intelligence analysis techniques, it is frequently possible to interpret or predict events based on open source usage. The evidence is often acquired through laborious textual analysis -- and by comparing media content with past actions.

- For example, FBIS analysts anticipated the February 1979 Chinese invasion of Vietnam by demonstrating that, with rare exceptions, the wording of authoritative Chinese warnings to Vietnam had only been used in instances in which Beijing had actually applied military force.

On some occasions, intelligence analysts adjudge open source information to be more accurate than classified sources. This can derive from either the weight and credibility of open sources versus the untested, contradictory or poor performing nature of the classified sources or from some other evaluation criteria. When we do favor unclassified sources over classified sources, we need to be sensitive to the credibility we have lent the data by adopting it as our own position.

Most people in our business agree that open sources have proven to be enormously invaluable to intelligence. Even during the Cold War, when intelligence was focused principally on acquiring secret information, open sources gave us some highly usable glimpses into closed societies. Today, with a generally more open world and a considerably more free and independent world press, open sources have even greater value for intelligence. In the new global environment, open sources provide much more hard, credible data about a wide range of international political, social, and economic issues.

There is a complex relationship between the way open source material is mixed with classified data and the concept of openness. We frequently have products where only a small amount of the overall data comes from classified sources requiring security protection. We have security procedures in effect to clearly mark paragraphs which possess classified data, and this enables much greater sanitization of intelligence publications to the unclassified level. The more complete and expansive the open sources, the more likely we can produce a wider variety of unclassified or lower classification products using the classified data as background for confidence-building and credibility. It is important to recognize that once an Intelligence Community agency puts its name on an essentially unclassified product, it may assume an enhanced credibility beyond that of the original open sources. This obligates the Intelligence Community to high standards of quality control, which we would expect of our people, in any case.

The Intelligence Community's current challenge is to expand the use of open sources to cover a broader range of issues -- such as weapons proliferation, economic competitiveness, and the environment. As one example, it is estimated that some 80% of the information needs for environmental intelligence can be met through information that is available to the public.

An you are well aware, the quality and quantity of open source information continues to grow:

- We have identified some 8,000 commercial data bases -- and the vast majority have potential intelligence value.

- The number of worldwide periodicals has grown from 70,000 in 1972 to 116,000 last year.
- The explosion of open source information is most apparent in the Commonwealth of Independent States, where today, there are some 1,700 newspapers that were not published three years ago.
- While the number of TV and radio stations around the world has not experienced rapid growth, the broadcast time and breadth and depth of their coverage, and the availability of cable TV are clearly on the upswing.
- The sources of "grey literature," (i.e., private or public symposia proceedings, and academic studies) around the world are also increasing dramatically.

As you know, open source encompasses a wide array of mediums -- including printed material, such as books, magazines and newspapers; as well as maps, photographs, data files, digital imagery and broadcast media -- both radio and television. These multimedia open source inputs correspond well to the range of product *outputs* used by the Intelligence Community. These intelligence outputs tend to be multimedia in nature, including hard copy and electronic dissemination of written and formatted, man and machine readable text, imagery, graphics, maps, and other situational displays as well as video. Because of the need to move data quickly in worst case situations, electronic information handling and display systems are most common. Most of these intelligence systems use off the shelf hardware, open systems, commercial architecture and operate as part of large area networks. The Intelligence Community has a special problem managing multilevel security in systems where open source data is mixed with classified data.

I'd like to say a special word about TV -- because it is a relatively new area for intelligence. Each week, FBIS monitors 790 hours of television from over 50 countries in 29 languages. Foreign TV programs -- such as news programs and documentaries -- give analysts a multidimensional feel for a country or material that other open source media cannot provide. Many analysts prefer to see the way a particular country chooses to portray events visually, rather than relying on the news network "filter." Coverage of foreign television brings us closer to what is happening in all areas of the world; it allows us to monitor crises as well as to broaden our knowledge of more restrictive societies. For example, the revolutions in Eastern Europe were covered extensively on those countries' domestic television.

In addition to analyzing foreign television, intelligence organizations are producing classified videos for policy makers which incorporate information from foreign news programs. The end result is a high-impact intelligence product used exclusively in the government that improves policymakers' understanding of complex issues.

The dramatic increase in open source material, its wide variety -- and its increasing value to intelligence -- demand a revolutionary change in the intelligence Community's approach to open source management, collection, processing and dissemination.

Unlike the other collection disciplines, which are highly structured, open source is not a tightly integrated discipline in the Intelligence Community. Over the years, open source information collectors, processors, and users have been diverse and decentralized groups spread across the breadth and depth of the Community. As a consequence, the various agencies in the Community didn't know the extent of unclassified holdings of other agencies, and had virtually no capability to share electronically the information which they did possess.

In short, the Community lacked a unifying structure, and a coherent and consistent set of overall requirements for the collection, processing, exploitation, and dissemination of open source information.

A DCI Task Force was formed last year to make recommendations on these issues -- and important changes are underway. As a result of the task force, for the first time the DCI has established an Open Source Coordinator (Paul Wallner of the Defense intelligence Agency) who is:

- cataloging the open source holdings of the Community as a whole;
- establishing a comprehensive requirements system for the Community; and
- establishing interconnectivity so open source information can be shared throughout the Community.

Another responsibility of the Open Source Coordinator is to interact with the managers of the other collection disciplines to ensure that they are not collecting against requirements that can be satisfied through open source materials.

In my view -- and this is a view shared by many throughout the Community -- open sources should be the Community's first step in a range of choices to meet our overall information needs. Compared to information collected from satellite and other reconnaissance and surveillance means, open sources are relatively inexpensive to acquire. It would be both bad acquisition management and information management to waste a costly intelligence asset collecting information that can be acquired through an open source.

Although I believe that open source should be the Community's first step in attempting to satisfy our information needs, I want to emphasize that it will likely never replace the other intelligence collection disciplines. But I do strongly believe that better and complementary management of open source assets will, in turn, lead to more efficient and focused use of those other collection disciplines.

Without question, the biggest challenge the Intelligence Community faces with respect to open source is processing the vast amount of data available.

Intelligence organizations have significant expertise processing and filtering large quantities of data, putting it on mass storage, manipulating it (including translation or gisting), and devising systems to have data available to analysts on an on-call basis.

In fact, US intelligence operates what is probably the largest information processing environment in the world. Consider this: Just one intelligence collection system alone can generate a million inputs *per half hour*; filters throw away all but 6500 inputs; only 1,000 inputs meet forwarding criteria; 10 inputs are normally selected by analysts and only one report is produced. These are routine statistics for a number of intelligence collection and analysis systems which collect to technical intelligence.

In the open source arena, FBIS monitors over 3,500 publications in 55 foreign languages. And each day it collects a half a million words from its field offices around the world and another half a million words from independent contractors in the US -- that's equivalent to processing several copies of *War and Peace* every day.

These two examples show the magnitude of the classified data and translation problems facing an already data-rich Intelligence Community. The open source challenge can theoretically present ever more daunting levels of data and translation requirements, reaffirming that information management will be the single most important problem for the Intelligence Community to address for the future.

In this equation, one of the dilemmas posed deals with how we will spread our already overtaxed Intelligence Community information management resources in the context of both people and systems across both the classified and open source collection and analysis areas. This conference can hopefully provide some pointers to solutions in this area, mindful of the fact that we are in a period of intelligence budget austerity and Community downsizing.

Of course, the key issue for intelligence analysts is not simply the quantity of open source data that is collected, but also its quality -- that is, its intelligence value.

Open source information is produced or published largely according to the needs of the private sector, without regard to the uses to which that information will be put by the intelligence customers.

At the present time, open source materials that are collected for intelligence are often not made available to analysts in a way that is useful to them. And there is only limited ability to search large open source holdings in a timely manner.

A substantial amount of open source information is reported in foreign languages and require translation. For example, in FY '92, FBIS translated 200 million words-- so the translation issue is another dimension to the information management challenge.

Much of the Intelligence Community's current open source architecture was developed in an age when information processing and communication were in their infancy. As we look to the future, we will have to develop more creative approaches to manage the vast amount of data being produced.

Based on the recommendation of the DCI Task Force, the Community-wide Open Source Steering Council has developed a Strategic Plan that presents a vision of the intelligence Community's goals for open source collection ten years from now.

The plan establishes the goal of creating an integrated Community open source architecture. The new architecture must provide, among other things:

- flexible collection,
- networked access to external data bases,
- immediate user and customer feedback, and
- automated, profiled delivery of collected open source information based on user requirements.

We expect the centerpiece of the architecture will be an Open Source Information Exchange -- comprising a central switch and digital communications networks which interconnect all user organizations within the Community.

The inputs to the Open Source Information Exchange will be government sources, such as the Library of Congress; the FBIS electronic dissemination system; and the vast array of commercial sources, such as NEXIS.

The system will distribute open source date through "functional support centers" that are being developed and funded by the Community. These functional support centers will serve as focal points of expertise on critical intelligence topics -- such as science and technology; and political, military, and economic intelligence.

The strategic plan begins with a vision for timely access to open source data, and identifies funding, management, and architecture considerations. It also establishes strategies and out-year timetables for open Source Coordinator pursuit of a more integrated open source design and implementation effort to support the widest variety of Community analysts and policymakers. Finally, it deals with specific requirements, collection, processing, exploitation, dissemination-related goals and objectives in specific detail. The plan is ultimately a roadmap for Intelligence Community-wide transition from the current way of doing business to future mode of operation. Its principal features bring us:

- from partial connectivity to full interconnectivity;
- from reliance on hard copy to digital electronic data;
- from dependence on physical information centers to the establishment of electronically-connected, virtual information exchanges;
- from querying one data source at a time to querying many at once;
- from the use of multiple standards and tools to common standards and tools;
- from development of sophisticated data bases on only a few topics to the creation of a wide range of data bases on many subjects;
- from limited access by users to sources of data to broad, flexible access;
- from emphasis on the collection and dissemination of data to a balance between that and making data readily accessible and tailored to user and customer needs;
- from a limited ability to display data to the ultimate application of fast developing multimedia capabilities.

Many important questions must be considered along the way. Open source is being considered by the DCI as the equivalent of a dominant intelligence discipline. in the restructuring of national intelligence, we have structural agency czars who are focused on and accountable for the management of national disciplines; for example, NSA for SIGINT, CIO for Imagery and the CIA/DO for HUMINT. Open source is far more decentralized in its current and even its envisional approach and management. *Will* the time come when we need more focus and accountability in open source management, mandating the establishment of a structural czar for this critical area?

How will we change the mindset of those people in the Community who do not yet think of open source as a bona fide collection discipline on a par with SIGINT or IMINT, or HUMINT?

There is no question that open source -- in comparison with other collection systems -- has the potential to provide a lower cost, lower risk supplement to intelligence collection and analysis. But access to open source data still costs money. So another question the Community will have to consider is, "Just how much money will be available to spend on managing open source data in an era of potentially *dramatically* declining resources?"

An expanded use of open source material raises legal questions -- especially concerning licensing agreements and copyright protection. Lawyers and managers in the Intelligence Community are working diligently to ensure that our use of copyrighted information strikes the appropriate balance between the government's legitimate need for access to open source material with the copyright owners rights and privileges.

For instance, the Intelligence Community, like any other commercial user, buys access to a number of commercial data bases. When one component of the Community is licensed to use a data base, can it disseminate that data, or provide access to other users in the Community? If the answer is not clear, we work with our commercial vendors to revise our basic agreement to ensure that our use of the material is consistent with our agreements with the vendor.

I would like to conclude by reminding you that the great strength of American intelligence, which is unique in the world, is its ability to responsibly manage a global intelligence system, continuously moving bits of data from diverse sources to a broad and demanding customer-set. That new customer-set has even more highly distributed information requirements for the future.

Fundamentally, it is the hundreds of messages and other intelligence products that we electronically disseminate hourly which constitute the bread and butter of the intelligence business. Our implicit requirement is to manage a virtual intelligence system which adapts its multimedia products to the demanding users in a changing and unsettled world environment. Open source material fits legitimately and prominently into the equation of modern intelligence sources and methods, but presents special challenges and dilemmas for us to resolve.

Well, that's a lot to think about -- and I can assure you that the Intelligence Community is well aware of the opportunities -- and the challenges -- associated with open source in our world today and of tomorrow. And we plan to draw on the expertise of the private sector, other government agencies, and the academic community to meet these challenges in the years ahead.

This conference is just one way we can help to make all this happen. Thank you for your interest in this important topic; we look forward to continuing to work with you in the future as we attempt to address these and other problems associated with the provision of focused intelligence and information support to our customers in a changed and changing world. Thank you for the opportunity to be with you today, and I wish you well for the remainder of this timely and important conference.

OPEN SOURCE INTELLIGENCE: WHAT IS IT? WHY IS IT IMPORTANT TO THE MILITARY?

Robert D. Steele, President OPEN SOURCE SOLUTIONS, Inc.
http://www.oss.net/

Introduction

This White Paper defines Open Source Intelligence (OSCINT) and its relevance in meeting the needs of the military (both commanders and defense policy-makers).

OSCINT is intelligence derived from public information--tailored intelligence which is based on information which can be obtained legally and ethically from public sources.

This White Paper suggests that OSCINT is a both force multiplier and a resource multiplier. OSCINT provides a practical political and military advantage which complements the advantage provided by traditional intelligence, it is available at low cost, and it cannot be ignored.

First the paper describes and discusses the utility of OSCINT in general terms, and at the strategic, operational, tactical and technical levels of warfare, including a single practical example at each level. The paper then describes the "information continuum" within which a range of open sources, systems, and services can be obtained which are relevant to military needs. Finally, the paper provides a brief discussion of the status of the open source intelligence programs in tile United States, The Netherlands, and Sweden, and concludes with a concise discussion of opportunities and risks inherent in the use of OSCINT to meet military requirements, and of several practical steps that can be taken to exploit OSCINT in support of military strategy, operations, tactics, and technical acquisition and countermeasures.

The official definition of OSCINT by the U.S. Intelligence Community:

> By Open Source we refer to publicly available information appearing in print or electronic form. Open Source information may be transmitted through radio, television, and newspapers, or it may be distributed by commercial databases, electronic mail networks, or portable electronic media such as CD- ROM's. it may be disseminated to a broad public, as are the mass media, or to a more select audience, such as grey literature, which includes conference proceedings, company shareholder reports, and local telephone directories. Whatever form it takes, Open Source involves no information that is: classified at its origin; is subject to proprietary constraints (other than copyright); is the product of sensitive contacts with U.S. or foreign persons; or is acquired through clandestine or covert means.

The official definition is limited in its understanding to standard commercial sources of traditional information, and excludes, to take one important example, SPOT imagery. It also fails to take into account the importance of unpublished materials including electronic information and human knowledge which can be accessed legally and ethically.

The official approach to OSCINT is also limited in that the existing information- handling architectures for intelligence processing, including dissemination to the commander, are all classified, and there is a very limited capability for routing unclassified information efficiently, even assuming it can be obtained. In most communities, there appears to be a

reluctance to assume primary responsibility for the collection and processing of OSCINT, which is why military operators in two countries (the United States and the United Kingdom) are examining means of acquiring and exploiting OSCINT directly, bypassing the intelligence community in order to give action officers at the policy level, and commanders at the operational level, direct access to OSCINT.

Experienced intelligence professionals have found that while OSCINT is not a substitute for traditional intelligence disciplines, including Human Intelligence, Imagery Intelligence, and Signals Intelligence. However, OSCINT does offer three major advantages for planning and conducting military operations:

- When encountering requirements for military operations in the Third World or in support of humanitarian assistance and counter-terrorist operations for which intelligence collection priorities have not been high, OSCINT is frequently the only discipline able to respond rapidly (to include commercial imagery), and it provides the commander and his staff with a rapid orientation adequate for both developing initial planning packages; and for establishing collection requirements for the traditional intelligence disciplines.

- OSCINT is also a means of achieving significant savings, in that many essential elements of information required by the commander and his staff can be acquired from commercial sources at a lower cost, m less time, than from classified capabilities, with the added advantages that OSCINT is often more up to date, and requires no political risk in its acquisition. This permits classified intelligence capabilities to be focused quickly and effectively on mission-critical gaps, and avoids depleting or misdirecting these scarce resources-- "do not send a spy where a schoolboy can go".

- Finally, OSCINT, whether it precedes or follows traditional intelligence collection, can protect national intelligence sources and methods by serving as the foundation for intelligence support to joint and coalition operations where it is not possible, or desirable, to reveal tile capabilities and limitations of the traditional intelligence community.

Open Source Intelligence and the Military

The availability and utility of OSCINT depends upon, and will vary, depending on the specific area of operations under consideration, and on two other factors: the level of warfare, and the point on the spectrum of conflict, from presence to general war, where the intelligence will be applied.

In general terms, OSCINT has significant potential as a source of intelligence support in terms of indications & warning, policy development, contingency planning, security assistance, weapon acquisition (design and countermeasures), joint and coalition operations, and tactical operations against new priorities such as proliferation. Finally, OSCINT is vital as a means of rapidly orienting the commander and serving as the foundation for collection management within the traditional intelligence disciplines.

At the strategic level:

- OSCINT can provide indications & warning of both hostile intent, and opportunities for military advantage. Content analysis of multiple open sources such as regional newspapers from tile Middle East, are often if not always more reliable foundations for estimating stability and instability, than reports from clandestine sources with a limited range of access and a personal perspective that biases their reporting.2 OSCINT is especially valuable with respect to cultural and demographic intelligence, areas not generally well- covered by traditional civilian and military intelligence collection and analysis capabilities.

- OSCINT can also provide very important geographic and civil generalizations which can significantly affect major military acquisition and design decisions. For instance, most countries build their aircraft for optimal performance on a "standard aviation day" which is defined in terms of warm (60-7O degrees) conditions and balanced humidity. The military commander that is responsible for expeditionary operations to the Third World will find themselves utilizing aircraft which carry half as much half as far because the standard aviation day in the Third World is hot (over 80T with high humidity). If aircraft cannot be designed for optimal performance on a hot day, then the military commander can at least ensure that doctrinal publications reflect accurate load and lift capabilities for the true expeditionary conditions to be encountered.

- OSCINT can provide unclassified threat intelligence which can be used to educate and mobilize public and political support for military needs including policy development.

At the operational level:

- OSCINT can provide the geographic and civil generalizations required for regional force planning and force employment. In particular, OSCINT has establish credible regional generalization regarding the capabilities of air, ground, and sea forces to be encountered by tile commander; geographic generalizations with respect to cross-country mobility, average line of sight distances, temperatures, and water availability; and civil generalizations such as bridge-loading, port clearance, airhead bunkerage; and civil communications and computing resources. OSCINT provides a time-sensitive solution to questions the theater commander will have about civil infrastructure, political cliques and personalities, and economic or financial factors affecting operational employment of forces, and is therefore especially helpful to contingency planning which must be pursued without adequate support from traditional intelligence capabilities.

- OSCINT is especially useful to the theater commander for the coordination of joint and coalition operations where traditional classified intelligence capabilities are either not available (e.g. in much of the Third World where lower priorities have restricted coverage), or cannot be shared with foreign elements.

At the tactical level:

- OSCINT has been shown to be highly pertinent and effective against new priorities, including counter-proliferation, counter terrorism, and peacekeeping operations. This

is true for both conventional military operations focused on overt interdiction, and clandestine or covert "direct action" by special operations forces.3

- OSCINT is a critical resource for the military commander who requires maps and digital targeting information for Third World area for which current geographic information is not available from government sources, whether classified or unclassified. In combination, SPOT and other commercial imagery resources can provide the commander with up to date maps containing all airfields, roads, and bridges; and soon containing contour lines as well, for expeditionary operations.4

At the technical level:

- OSCINT about civil communications and computing capabilities in the area of operations will be very important to the commander. As information warfare and information peacekeeping become critical mission areas, and all opponents achieve some capabilities to conduct electronic warfare, the commander will need to use OSCINT both to understand how to degrade the performance of civil capabilities being used by opponents, and to consider exploitation of civil capabilities to maintain joint and coalition communications.

- OSCINT will provide most of what the commander needs to plan and coordinate joint and combined air, sea, and land operations in the expeditionary environment, with specific reference to strategic airlift and sealift operations involving civil aircraft, air traffic control and air defense planning for civil platforms, and fueling and other logistical considerations.

The Information Continuum

There are three ways of understanding the robust nature of the private sector's potential contribution to military intelligence needs. The first is by examining in general terms this continuum.

		Private Investigators		
Schools	Libraries	Information Brokers	Government	Intelligence
	Universities	Businesses	Media	Defense

Each of these nine sectors of the global or national information community maintains a cadre of human experts as well as a range of both hard-copy and electronic information. Much of what is known to them, or stored by them, is not available through commercial online services. Following a specific example from each sector:

- Language schools can rapidly identify individuals by location and nationality who have received trailing in the home country language and are target country nationals (e.g. Somalis studying French in Paris); these individuals can be contacted and offered part-time employment as translators.

- Universities utilize their existing infrastructures and a regular supply of cheap intellectual labor to maintain important and authoritative databases. The Monterey Institute of International Studies, for instance, maintains the best database on the

proliferation of nuclear materials, and utilizes graduate students fluent in Russian, Chinese,. Arabic, and other languages to cover a wide range of multi-lingual publications, and to maintain an electronic database, at very low cost.

- Libraries can be used, either as needed or in a deliberate fashion, to serve as repositories for "just in case" archiving of political-military, economic, and other materials pertaining to specific countries. This allows the government to share the cost of archiving with other library sponsors, and in many cases avoid the cost all-together.

- Businesses have enormous repositories of market research, including communications and logistics research, on countries throughout the world where they have made or plan to make an investment. Businesses are also acutely familiar with the political corruption, climate conditions, and other factors which affect operational efficiency in specific locations. Two unique examples of business dedicated to meeting private intelligence needs are Oxford Analytica, with its network of 750 overt agents world-wide, and The Economist Intelligence Unit.

- Information brokers can be identified who specialize in particular scientific & technical topics or regions of the world. This permits more efficient search & retrieval by exploiting capabilities whose "learning curve" has been funded by others. In addition, information brokers can be identified with specific language capabilities, and employed to do rapid exploitation of captured or acquired documents.

- Journalists responsible for specific areas of the world, including journalists specializing in military, aerospace, and insurgency matters, rarely publish ten per cent of what they know, and they never publish their sources. They can, however, be engaged to prepare special reports, and to provide background information on specific personalities of importance to planned military operations. This need not be done secretly or through direct recruitment; it can be done discreetly as a private commercial transaction. Media organizations, such as Jane's Information Group, acknowledge that they publish less than 20% of what they know, in some cases to protect sources--they are however willing to do tailored confidential reports drawing on their complete range of sources.

- Governments, including provincial and state governments, frequently have experts in agriculture or other trade-related fields who are familiar with specific areas of operation and the logistics as well as the key personalities. Embassies have personnel whose reporting does not fully communicate what they know. Bringing key government personnel together for a week can quickly establish a foundation for collection management which the commander could not normally achieve through analysis of raw information.

- Other intelligence organizations, including the "information and research" elements of tile Vatican, the United Nations, and the International Red Cross, have global networks of reporting sources, including sources with special linguistic and regional skill, that can be drawn upon.

The third way of understanding the robust capability of the private sector is to consider the range of information services that are offered which are directly pertinent to military intelligence needs. These are listed in three columns:

Direct Observation	Document Acquisition	Telephone Surveys
Commercial Online Searching	Document Translation	Market Research
Current Awareness	Broadcast Translation	Recruited Agents
Experts On Demand	Multi-Expert Research	Industrial Espionage

Recruited agents and industrial espionage are not considered legal nor ethical within the private sector, but there are very competent organizations that openly offer such services, to include route reconnaissance and target identification services in third countries. In each of the above categories, it is highly likely that a private sector partner can collect, process, translate, and deliver open sources of intelligence able to make an important contribution to the commander's needs for information--and to do so in a cost-effective fashion which could not be duplicated by defense attaches or traditional military intelligence collection brigades.

The third way to understand the utility of the private sector for military intelligence needs is to take a case study, such as Somalia. In. the absence of internally-available intelligence information, the fastest means of establishing an encyclopedic foundation for further collection management, and the fastest means of providing the commander with at least some useful information pending responses from the traditional intelligence disciplines, it by seeking out private sector experts and private sector databases. A leading scholar, a leading businessman recently returned from a tour as General Manager in Somalia, a leading journalists, and perhaps an information broker specializing in African information could be brought together and could quickly identify human, hard-copy, and electronic sources--including sources of digital geographic information--of immediate utility.

In one specific instance, supporting a wargame on Somalia, an individual playing the role of the United Nations commander was able to overcome the inadequacies of the U.S. intelligence community by making three telephone calls. Overnight, in Express Mail, at a pro forma cost of about $5,000, the individual received:

- From Jane's Information Group, a spiral-bound volume containing a map of Somalia clearly marking the nine clan areas; a one-page order of battle for each clan (at a time when most intelligence analysts were thanking only of the old Somali army); and a one- paragraph précis with full citation for each article about Somalia published in any of the Jane's publications (including the excellent Jane '5 Intelligence Review) in the past two years. This constituted a superb orientation for both planning and collection management.

- From Oxford Analytica, twenty two page reports suitable for Presidents and Prime Ministers, covering three topical areas: United Nations operations in Somalia, U.S.

foreign policy toward Somalia; and U.S. operations related to Somalia. Again, a superb orientation on strategy and policy, in concise and immediately-usable form.

- From The Economist Intelligence Unit, a copy of the appropriate country risk report, which included important summary information on the logistics difficulties that would be encountered, including the limitations of both the port and the airfields for strategic entry.

Commentary on Representative National Approaches to OSCINT

Although OSCINT has always been part of the national and military intelligence process, in recent decades increased emphasis on technical systems and secret collection have tended to sharply reduce the amount of funding and the number of personnel dedicated to collecting and processing publicly available information. At the same time, the "information explosion" or "information revolution" has dramatically increased both the quality and quantity of the information available in the public sector. Today the commander can take a weather map of Bosnia off of the internet, or exchange email with volunteer observation and listening posts in Bosnia.

Unfortunately, the reality today is that most intelligence communities are trained, equipped, and organized to collect and process secrets. OSCINT capabilities in both the civilian and military sectors of government have both atrophied where they existed, and also failed to keep up with the growth of private sector OSCINT capabilities.

- United States of America. The National Foreign intelligence Board was recently briefed to the effect that while 99% of the $28-35 billion dollars a year budget is spent on classified collection and processing, and only 1 % is spent on OSCINT, OSCINT provides 40% of the all-source product. in one interview, the Deputy Director for Science & Technology of the Central Intelligence Agency stated that this latter figure was actually 70%. The major element of the U.S. intelligence community program is the Foreign Broadcast Information Service, which is under severe criticism for its continued emphasis on print media exploitation, and its inability to master a wider range of open sources. in an attempt to gain control over the modest distributed resources being applied to OSCINT, the Director of Central intelligence created the Community Open Source Program Office. This office is about to release a strategic plan for OSCINT, but it is limited to improving internal community access to open sources already collected. The Department of Defense program, for which the National Air Intelligence Center is the executive agent, builds on the existing scientific & technical intelligence document acquisition and translation program. The Department of Energy laboratories, and especially Sandia and Los Alamos, constitute a major OSCINT resource which is being exploited by some military consumers of intelligence, such as the U.S. Southern Command, but which is not under the control of the intelligence community. Some very modest individual initiatives have taken place within the military services, the most advanced of which is the publication, in draft form by the Army, of an open source primer for military intelligence officers. At this time the U.S. military does not have timely broad access to a full range of open sources.5

- The Netherlands. Various open sources, including the Intelligence Newsletter out of Paris, and OSS NOTICES in the United States, have reported that the foreign and

military intelligence agencies have been integrated. Within the new national intelligence agency, a special Open Source Coordinator has been appointed, and a task force approach is being taken to intelligence collection and analysis. Every task force has an open source intelligence specialist, and all requirements for intelligence must first be examined and if possible satisfied through OSCINT before tasking of clandestine or technical capabilities is permitted. More recently, the intelligence elements of the individual military services were integrated into a joint military organization reporting to the Prime Minister.

- Sweden. This country is most interesting because is has a unique consortium within which to formally orchestrate the activities of government intelligence, the business intelligence community, and the university research community. Swedish scientific & technical attaches have been noted to regularly exploit the internet, and there is discussion within Lund University of the need for an Open Source intelligence Center to meet the combined needs of the government, business, and university communities in Sweden.

Advantages and Disadvantages of Open Source intelligence

Advantages include the fact that OSCINT has virtually unlimited potential on any topic; is of relatively low cost because expertise is maintained at someone else's expense; is generally up to date; and can be shared with anyone.

Disadvantages include the possibility of revealing military plans and intentions (security can be provided by laundering the question through trusted intermediaries); the time and cost associated with searching for exactly the right information within the huge volumes of public information; and the temptation to accept an open source at face value when it could be disinformation or simply inaccurate.

Obstacles to Military Exploitation of Open Sources

There are three obstacles to military exploitation of OSCINT:

- Organizationally, the military relies on a classified intelligence community for its "intelligence", and does not have an alternate structure established to obtain OSCINT. Among the most important problems created by this reliance are those of funding: there are no well-established programs for contracting directly with the private sector for OSCINT.

- Culturally, there is a strong attitude, primarily within the intelligence community but to an extent within the operational community, that information achieves a special value only if it is classified. This is in part a result of a cultural inclination to treat knowledge as power, and to withhold knowledge from others as a means of protecting one's power. This attitude is the equivalent of the Calvary ignoring the tank and the machine gun. The "openness" paradigm has thoroughly defeated the secrecy paradigm, and those organizations which focus on protecting secrets rather than exploiting publicly available information, will find themselves "starving" for knowledge.

- Technically, because of the historical focus on training, equipping, and organizing forces for unilateral and conventional military operations, with the added assumption that all "intelligence" will come through classified and well-established channels, the existing command & control architecture, including communications, computing, and intelligence elements, is not designed to rapidly interface with joint and coalition forces, with special forces and direct action clandestine teams, and with the vast array of private sector and non- military government elements which can provide OSCINT to the commander.

Opportunities for Advantage

The Director of Military Intelligence (DM1) for any nation has essentially three opportunities to improve national capabilities to collect, process, and disseminate OSCINT to commanders and military policy-makers:

- Existing library resources are poorly-funded and organized for the purpose of "just in time" archiving of information. Library resources, both within the intelligence community and outside the intelligence community, must be recognized as the "source of first resort"6 Commanders and policy-makers must restore funding for library operations, including the cost of subscribing to external online services and out-sourced research, while at the same time redirect the libraries toward '"just in time" decision-support to specific consumers, and away from '"just in case" generic collection and processing.

- Existing military intelligence analysts must be given the training, fiscal authority, and commander's guidance necessary to convert them from narrow specialists focusing on the analysis of classified information, to managers of networks of overt human experts and related electronic and hard-copy databases. At the same time, analysts must be re-oriented so that their primary focus is on day to day interaction with the commander and other consumers of military intelligence, and on day to day collection management founded upon open source exploitation, rather than the existing focus on producing classified reports in isolation from the consumer.

- Existing commanders, in consultation with the DM1, must recognize that it is impossible for the DM1 to satisfy their intelligence requirements related to a wide range of new priorities, with existing classified military intelligence capabilities. The entire structure of military intelligence must be recast to permit rapid maneuver throughout the private sector's knowledge terrain, and the rapid collection, processing, and dissemination of mission-critical OSCINT to the commander at every level of operations (strategic, operational, tactical, and technical) and in "every clime and place".

Role of the Military Reserve

The military reserve constitute a national resource which has enormous potential. A simple example will serve to make the point. For every country of interest, a cadre of five military intelligence reservists could be formed, and given a responsibility to monitor pertinent foreign language periodicals and publications (which would be provided them on subscription), and to prepare weekly OSCINT summaries. These same individuals should be afforded direct access to the Internet and commercial online databases, and serve as direct

reinforcements on demand to the active duty military intelligence analysts responsible for the same areas of interest. Funds should also be provided for the five person cadre to spend thirty days each in the country of interest, unencumbered by administrative duties. In this way, when a contingency requirement emerges, the responsible commander can activate the appropriate cadre (or cadres in the case of a theater commander).

Endnotes

1. Although the original intelligence community report was classified SECRET, the definition and extensive commentary appeared in an unclassified document, United States Marine Corps Comments on Joint Open Source Task Force Report and Recommendations (Working Group Draft Dated 6 January 1992), and portions, including the definition, were subsequently reprinted in OSS NOTICES Volume 2 Issue 9 (30 November 1994).
2. This point was made publicly by Dr. Stephen Fairbanks, the Iranian Analyst for the U.S. Department of State's intelligence and Research Bureau, in the presence of his superior, Dr. Jennifer Sims, Deputy Assistant Secretary of State for intelligence Coordination.
3. At a Canadian intelligence conference 27-29 October 1994, both the Director of the Canadian Security and intelligence Service, Mr. Ward Elcock; and Dr. Paula Scalingi of the Los Alamos National Laboratory in the United States, stated that OSCINT provides over 80% of the input to the final all-source product; in Dr. Scalingi's case, this was with specific reference to intelligence support for counter-proliferation. Dr. Gordon Oehler, Director of the U.S. Intelligence Community's Nonproliferation Center, has made similar comments on several public occasions.
4. SPOT is going to 5-meter resolution imagery in the very near future. in the U.S. Space Imaging, Inc., a subsidiary of Lockheed, has announced plans to provide 1:2,500 meter synoptic resolution imagery, within a year. These commercial capabilities will be critical to expeditionary operations in the Third World because of the lack of current maps. One U.S. study, Overview of Planning and Programming Factors for Expeditionary Operations in the Third World (Marine Corps Combat Development Command, March 1991), determined that for the 69 countries of concern to the Marine Corps, there were no 1:50,000 combat charts for 22 of the countries, old 1:50,000 charts for ports and capital cities only in the case of another 37 countries, and very old 1:50,000 complete coverage for another ten countries.
5. The extraordinary relevance of Department of Energy OSCINT capabilities in support of military operations are described in SHARING THE SECRET: Open Source intelligence and the War on Drugs (OSS inc. Limited Edition, 1994). The Army paper, prepared by the 434th Military intelligence Detachment, Strategic, is tided Open Source intelligence Resources for the Military Intelligence Officer (Fort Huachuca, November 1994).
6. This important phrase was developed by Mr. Paul Wallner, the first (and last) Open Source Coordinator in the Office of the Director of Central intelligence in the United States. Mr. Waliner, a member of the Senior Executive Service (flag rank) served for many years in the Defense intelligence Agency and has been a strong advocate for improving OSCINT support to the commander. Today he serves as Deputy to the first Director of Community Open Source Program Office, Dr. Joseph Markowitz.

THE PRIVATISATION OF INTELLIGENCE: A WAY FORWARD FOR EUROPEAN INTELLIGENCE COOPERATION - "TOWARDS A EUROPEAN INTELLIGENCE POLICY"

Dr Andrew Rathmell
RAND Europe, http://www.randeurope.org/

Introduction

A major objection to increasing international cooperation in the intelligence field is the traditional reluctance of intelligence services to share information on their sources and methods. At the other end of the intelligence "chain," nation states have also been reluctant to rely on their allies for the all source assessments on which, ultimately, political and diplomatic policy are based.

Despite the growth of trans-European intelligence networking, these sensitivities will continue to hamper efforts to improve intelligence collaboration in a European framework. The argument of this paper, however, is that the "privatisation of intelligence" in the developed world will help to break down such barriers to cooperation and provide means by which all European states can benefit from pooling resources. Critically, budgetary pressures will push collaboration while the pull of privatised intelligence will encourage outsourcing and make collaboration easier.

Privatising Intelligence

Intelligence services have always made extensive use of "open sources" - from studying foreign press to debriefing businessmen and tourists and collaborating with academics and scholars. Proponents of the Open Source Intelligence (OSINT) revolution however argue that the intelligence business has been revolutionised at the end of the twentieth century by the information revolution that has generated a flood of data available without recourse to clandestine methods.

This paper accepts that intelligence services can now glean increasing amounts of data from open sources but argues that the privatisation of intelligence for European governments in the 1990s goes further than this. The privatisation of intelligence includes four components: targets, sources, methods and costs.

Targets

The geopolitical changes since the end of the Cold War and changing attitudes to the role of Western military forces and European global security interests have changed the intelligence targets of concern. European agencies must focus on a much wider range of potential targets, all of which are individually of a lower priority than the Warsaw Pact during the Cold War. They must now pay attention to arms proliferation, terrorism, crisis prevention and monitoring and prepare for possible military intervention overseas, whether humanitarian or otherwise. Although certain key issues, such as WMD programmes in certain states or the

activities of certain terrorist groups, will require consistent and in-depth monitoring, other issues will require a broad-brush overview combined with a surge capability.

This broad brush overview can often be provided by open sources (e.g. press, media, individual experts, diplomatic reporting). At the same time, there is a convergence of interests between defence intelligence services on the one hand and criminal intelligence services on the other in the fields of, for instance, organised crime. Both sides of the fence are not only having to learn from each other's experts but are rapidly having to educate their personnel in relation to their new targets. This is the stage at which OSINT and expertise is often the most useful.

Sources

As Robert Steele and others have argued, the information revolution and the proliferation of media and research outlets mean that much of a state's intelligence requirements can today be satisfied by a comprehensive monitoring of open sources. There is little reason to think that this can be done better by in-house experts than by established private sector research institutes and companies. Crucially too, outsourcing will often relieve budgetary pressures.

Not only are open sources now more widely available, but the information revolution is even blurring the boundaries between open and covert sources in regard to the formerly sacrosanct technical collection means. The proliferation of civil Earth Observation satellites and improvement in image analysis techniques are rapidly eroding the monopoly on Imagery Intelligence (IMINT) formerly reserved for the USA, Russia and, to a lesser extent, the PRC.

Methods

They key to good intelligence is all source assessment. While state apparatuses, especially in the major European military powers, have methods and mechanisms that cannot be matched by the private sector, these methods and mechanisms are optimised for certain core missions. Since these methods were designed around Cold War scenarios, they are not necessarily best placed to assess new threats and support new missions. Two areas of note are Operations Other Than War (OOTW) and Information Warfare (IW). The new complex of issues surrounding these contingencies involves less traditional hard military net assessments and diplomatic intelligence, and more soft analysis of complex political, paramilitary, social, economic and technological issues. Since these new issue areas are only now being defined and categorised, more flexible private sector institutions, less locked into established modes of analysis and less beholden to bureaucratic imperatives, can offer a lead in reformulating intelligence methodology for a new era.

Costs

As defence budgets shrink across Europe, armed forces are having to rethink their provision of in-house expertise. Britain has already decided to "privatise" the education of its staff officers in order both to save money and to improve quality. In terms of technology, armed forces are increasingly reliant on off the shelf technology (COTS) while many of the technological advances in the Revolution in Military Affairs (RMA) are now civilian and not military led. These processes are likely to continue; the logical corollary is an increasing reliance on OSINT. Importantly, the low level of classification required for such sources and

methods also enables resources to be pooled between states. This further reduces costs and is likely to improve European coordination in a time of crisis.

Sources and Methods: Satellites and Information Warriors

In order to put some flesh on the skeleton outlined above, this section considers two particular areas in which the information revolution is increasing the role of the private sector. The leading role of the private sector in these areas makes it much easier for European states to collaborate both to improve their intelligence take and to cut costs. First, I will discuss one type of intelligence source, space-based IMINT. Second, I will discuss the methodological issues related to Information Warfare.

The Earth Observation Revolution

A striking feature of modern international relations has been the impact of the dominance exerted by the USA in regard to the provision of satellite IMINT. America's vast investment in its space-based surveillance and recconaisance infrastructure has given it tremendous influence both diplomatically and militarily. Desire to break out of this hegemony has encouraged some states to pursue their own space-reconnaissance capabilities, such as the Helios and Japanese satellite programmes. Proponents of closer European intelligence collaboration often argue that it is necessary to enable Europe to afford to deploy its own high resolution surveillance satellites. However, the accelerating technical and market revolution in the civil Earth Observation (EO) field is providing capabilities that will soon enable the private sector to challenge the US hegemony in overhead imagery and provide IMINT capabilities unaffordable even with a joint European satellite programme.

The EO Revolution has four key components: Sources of Imagery, Quality of Imagery, Image Processing & Analysis techniques, Developments in Data Integration.

Sources of Imagery: Whereas SPOT and Landsat for many years were the sole commercial providers of imagery, other providers are now emerging. Already Russia and India market high quality imagery, as do Europe and Japan from the ERS and JERS radar satellites. By the turn of the century, perhaps three American companies will be providing electro-optical imagery while Canada will be selling data from its Radarsat. Europe will also be marketing data from its ENVISAT while Japan may market data from its proposed EO satellites. The impact of this proliferation of suppliers is to make data cheaper and data supply more reliable, meeting two of the key requirements of an intelligence service.

Quality of Imagery: Intelligence services are understandably keen to have high resolution imagery and have never considered Landsat, for example, of much significance due to its coarse resolution. The Very High Resolution electro-optical data now being marketed and being proposed means that sub-one metre resolution data will soon be available. This is adequate for most defence tasks. Moreover, the number of EO satellites in orbit and the variety of sensors available (panchromatic, Multi-Spectral, Synthetic Aperture Radar) can provide a level of coverage in terms of repeat times and in terms of elements of the spectral band that not even the US government has achieved.

Image Processing & Analysis techniques: Advances in civil applications of image processing for both electro-optical and radar data mean that more information than ever can be extracted from imagery and that data management issues can also be addressed. While classified

programmes within the US will continue to lead in some of these areas, industry and academia can add significant value to EO data, often at lower cost. In addition to technological developments, the skills and data required for this highly specialised type of intelligence gathering are proliferating into the private sector.

Developments in Data Integration: Overhead imagery can no longer be seen as aerial photo-recconaisance writ large. The emergence of data integration tools, such as Geographic Information Systems and Digital Terrain Modelling, marks a dramatic advance in the ability to generate maps and terrain models of unknown areas. In light of the probability that European forces will have to intervene at short notice in unfamiliar geographical areas, the benefits for mission planning from GIS and DTM are incalculable. Again, the data sources, the tools and techniques involved are being led by the private sector.

The EO Revolution has profound implications for the privatisation of intelligence and for European collaboration, some of which were recognised with the establishment of the WEU Satellite Centre. High quality overhead imagery will soon be available to all comers combined with greater than ever analytical and mapping capabilities. Although individual national intelligence services will obviously make use of these new capabilities, the fact that the sources and methods are "open" - available commercially, opens the way for them to be exploited collaboratively. This will reduce costs and increase synergy. The fact that these resources are not controlled by any one member state will remove the possibility of any disputes over tasking, as has happened on occasion with Helios.

Information Warfare

Information Warfare is still a contested term and has been given many different meanings. For the purposes of this paper, it is defined as "attacks on, or defence of, information activities." Although targeting an enemy's Command, Control and Communications (C3) is not new, the use of the term IW takes account of the fact that both militaries and states are increasingly reliant on Information Infrastructures to conduct their business. Although physical infrastructures (railway lines, bridges) remain critical, at least as important are critical nodes in Information Infrastructures.

An emerging concern among intelligence agencies therefore is to examine the implications of this reliance by armed forces and societies on networked communications. Even the USA, which has jumped onto the IW bandwagon, has not yet however conclusively defined its approach and methodology. European states have so far paid relatively limited attention to this topic. As they turn their attention to it, they will find it extremely beneficial to look to the private sector in three respects: Conceptualisation, Threat Assessment, Vulnerability Assessment.

Conceptualisation: For better or worse, America's conceptual approach to IW has been shaped by non-governmental "experts," such as the Tofflers. The lack of scholarly rigour evident in such popularised analyses is however widely acknowledged and it is evident that a great deal of hard intellectual work needs to be done in Europe to put IW in context and to develop the conceptual tools without which policy and doctrine will be incoherent and poorly grounded. Although such high level thinking is being done within government circles, there is a place for substantial input from the academic strategic studies community and from the academic/commercial Information Technology community. This early stage of conceptualisation requires a true partnership. At a later stage, when policies are being

implemented, this partnership will need to be formalised and extended. The USA, for instance, has explicitly structured its Computer Emergency Response Team (CERT) concept as a partnership between executive agencies and the private sector. Despite the massive expertise and resources of, for instance, the NSA, it has recognised that a partnership is the only viable option.

Threat Assessment: European intelligence agencies are only now beginning to develop threat assessment methodologies for IW. One pressing problem in assessing the extent and nature of the threat is the lack of data regarding "real-world" IW attacks, as opposed to speculations about the potential IW threat. It is commercial institutions that are in the front line of IW-type attacks, usually for criminal purposes. Government police and intelligence services have however found it very difficult to extract reliable information from companies about the extent of the damage inflicted. The aims of the two sides are often in opposition. Companies are concerned to avoid publicity which will impact on consumer confidence whereas governments are concerned at locating, understanding and neutralising the threats. To resolve this contradiction, there is place for more reliance on privatised intelligence.

For instance, in 1994 King's College carried out a threat assessment for UK-based companies considering the physical threat from the Provisional Irish Republican Army (PIRA). Despite the sensitive nature of the subject, it was established that a combination of research methodologies (strategic analysis and consumer threat perceptions) could usefully generate methods and data of benefit to both government and the private sector. Possibly more importantly, the research process provided a mechanism for improved information exchange between the public and private sectors. This approach could contribute significantly to the development of national and multinational IW threat assessments. An additional area in which privatised intelligence would score over government intelligence is in tracking IW doctrinal and technical developments in other states. For instance, foreign scientists are often more willing to collaborate in research efforts with other universities than with defence agencies or intelligence services.

Vulnerability Assessments: In assessing the vulnerabilities of a National Information Infrastructure (NII) or the Global Information Infrastructure (GII), intelligence services already recognise the prime importance of working with the private sector. No modern government can understand the potential weaknesses in its NII unless it works closely with, for instance, leading IT companies and service providers. These forms of collaborative research need to be extended on an international basis due to the interlinking of NIIs with regional and GIIs.

Implications for Europe

Improved European intelligence collaboration is rational from the perspective of the push, declining budgets require resource sharing, and of the pull, the increased demand for intelligence and the proliferation of sources and methods. Nonetheless, reluctance to divulge sources and methods will act as a brake on intensified collaboration. This paper has argued, however, that the ongoing "privatisation" of intelligence will ease these sensitivities since, in a private-sector led environment, sources and methods will be widely available. Specialised and highly classified collection and analysis methods will remain under official lock and key but the role of classified programmes is likely to be significantly reduced in the near future. In order to benefit from the ongoing information and intelligence revolutions, all European

states could only benefit from closer European collaboration, both between governments and with the private sector.

OPEN SOURCE - LESSONS LEARNED

Mats Bjore

During our early work in the late 1980's we began to realise that the way we access information as analysts had to change. Due to the ever-increasing volume of information, we had to focus our interests.

For every major or minor event in the world there often is at least 20 independent sources that are reporting on the very same event. The risk and possibility of misinformation or deception have grown, but the risk also has been reduced. It had become harder for the remote and closed areas of the world to keep things in secret and to fool it's own citizens with propaganda.

The different media types blend and soon it will be impossible to decide which type of communicator has delivered a certain stream of bits. The television set becomes a computer. You download your e-mail to your cellular telephone. You use your computer to monitor the local TV or radiobroadcast from Israel to Brazil. The satellite dish on your roof is a super high-speed connection to the INTERNET. The change is continuous, simultaneous, accelerated, and nonlinear—in one word: chaotic.

How does an organization organize the monitoring and analysis of events that affect its operations in a rapidly increasing flow of information? They can not attend to every event in its environment, but must select areas of priority, filter incoming data according to its interests, and for further refining and analysis.

One of the major problems today is how to say NO to the quantity of information delivered by emerging push and pull technologies and instead focus on the quality of information needed for analysis. The human interface is still needed.

Our open-source function still acts as a human filter, in order to ensure quality. This has the added benefit of keeping our stored volume of information within reason—thus ensuring our clients relevant and timely retrieval.

History

In 1990 two disparate needs arose that necessitated the use of unconventional sources and methods.

The Swedish Army Parachute Ranger School required pictures and information at the tactical level.

The Army Intelligence School needed open information in its task to disseminate threat assessments. Much of the available information was either classified or not relevant. With open sources, both requirements were satisfied.

One of the incidental lessons learned quickly became known as ASKINT (or Asking Intelligence). There was a need for up-to-date pictures of materiel.

Instead of attempting the traditional covert (time-consuming and very expensive) means of collection, letters were sent out to manufacturers asking for the requisite pictures—ASKINT.

Aerospatiale, among others, promptly sent not six but 53 pictures of its product line. Even the Russians responded: the tank factory in Omsk sent pictures of its latest T-80 model.

In 1993 the Military Intelligence & Security Service realised the need to adopt the methods developed at the Intelligence School, on the strategic level.

At the end of 1996 we introduced our global-access document database the so-called Infobank.

In mid-1997 we became an independent unit within the service.

Our daily work is focused on three major products

The Open Source Information Report, the INFOBANK for the Defense Forces HQ and the GLOBAL INFOBANK for our external customers. Among our external customers we have the MoD, the Foreign Ministry (including many embassies around the world), the National Defence University, the Regional Military Commands, and other members of the Swedish Administration. Infobank is the text collection of all digital OSI collected since 1993. It is indexed both manually and for full text retrieval. We combine the best of two worlds.

Method

The most important task of the day is the routine collection of monitored sources. This is sometimes a very tedious task but it is necessary in order to maintain the quality of our INFOBANK. Our goal is to find and use primary sources

Our team work from several different locations and from their home offices. In The use of LRRP (Long Range Reconnaissance Patrol) tactics is important. Several hours a day the LRRP scans the forefront of the INTERNET or any commercial online-service for new relevant sources and reports and map the location, content and development of valuable sites and services.

They LRRP must have very good knowledge of the organisation's basic needs, full clearance for the content and work of SIGINT and HUMINT in combination with an innate sense or feel of what will become important. This scouting function also serves as a sort of Help Desk for the analyst and the information miners.

Yes we use the human interface. We believe until proven otherwise that the Mark I Eyeball driven by a hungry, curious brain is superior to any binary agent. The Push technology or profiling system, we believe, make the analysts passive and their curiosity for "out of the normal picture" gets drowned in the bitstreams of endless hits in the profiling systems. And a profiling system as of today and the nearest future will only make the active and curious analyst frustrated. He or she want to know more, learn the details and the want do DISCOVER the information by their unique individual way of thinking.

If you are part of a large organisation with many LRRP, it is essential to coordinate pointers to locations to be searched, and to establish procedures to create the organisation's own

source pages- If you do so, you don't waste valuable time in the collection process or duplicate your efforts.

A LRRP must be of an analyst's breed. We tried to use computer whiz kids but in our experience, you must have people with very broad skills and education. **Computer skills are not important but language, sometimes unconventional intelligence and "organisations" skills are essential.**

In addition to the LRRP we use miners that collect the information and structure the information in our system. Structuring means that insight or meaning is obtained by matching and relating information from multiple sources so that some form of pattern or trend emerges. Structuring is achieved by creating information about information, for instance, how data are organised, related and used. Classification, indexes, tables of contents, and data models are some examples of filtering and the structuring of data. Some sort of structuring combined with a sufficient text retrieval system hold the most potential for the successful exploitation of information.

A great deal of important information is present on the net for only a short period of time. When you have identified a specific piece of information, you must capture it and store it in your own system. For as long as you continue to want that information, you continue to monitor the source. If you use a local indexing system, you also get the benefit of having the information searchable and useable.

Although sometimes valuable, **the Internet today is not a solution to the analyst's need for relevant, timely information** The Internet is changing by the minute. New sites appear at a breathtaking rate—one of the major online Internet catalogues receives 22,000 new listings every day. At the same time, many sites go away. Because it only takes a few minutes at a computer to change a site, they change regularly. This means that mastery of Internet information is extremely perishable. **On top of the vast amount of new material entering the Internet, its structure and essence are also changing. The look of the Internet has also changed dramatically. Text-only “gopher” sites are being replaced by graphics-laden and sometimes beautiful “web pages.” This transformation will continue for some time.**

New resources and methods appear and others fade away on a daily basis. Within a few years, the web is likely to stabilise. Once that happens the analyst's or the LRRP's collection of Internet ~bookmarks" will be nearly as valuable as personal contacts are now. The modern analyst must prepare for this. By exploring the web today and developing effective methods for finding and using electronic information, the analyst will be ready and competitive when the Internet finally does make the leap from luxury to necessity. But as a manager you probably don't want your analysts to surf away from their given daily assignments.

We have solved this need by giving our analysts free access to the INTERNET at home but not on every workstation at work. Every section has a common resource (our play-station) with a wide range of online service including the Internet. It is important to motivate and tease the analysts to be curious about Open Sources.

The rapid pace of development on the INFORMATION BATTLEGROUND demands a constant R&D effort in an Open Source-based organisation.

Organisations must have constantly evolving and changing systems. These changes may not always be visible to the analyst but the manager of an Open Source system must understand and direct them.

As a metaphor, one can take a photo of river or a rapid. The photo is a frozen projection but is very hard to describe in detail. You can paint a picture or write an essay about the river but you can not imagine how the waterfall will look in detail the next second, minute or decade. The only way to comprehend the flow of water is to dive into the water, follow the currents, and try to master it during the ride.

We think the same applies to Open Source. It is and will be a chaotic ride! You must actively take part in the process to understand the process; to have visions and to create new methods and applications. In these areas, specialised R&D institutions are phenomena of the past.

If you have the resources, you must incorporate the R&D functions in the actual living Open Source-process. Your organisation soon will be a **knowledge-organisation** where changes can be very rapid but invisible in the daily tasks. If everyone can influence his bit of the process, the word **changes** soon will loose its meaning

We focus our collection on primary sources, and only use secondary sources when we have to. Often, however, secondary sources can be helpful in finding primary sources.

By using cheap technology and striving for information quality, we could afford to do mistakes. Our OSI organisation has its origin in tactical military intelligence and the same methods for collecting, structuring, analysing, and dissemination was applied to the operational and strategic level in both the military and in the field of security politics. We learn by trial and error.

For strategic analysts, the ability to collect information rapidly and to evaluate its relevance and validity is a crucial skill.. One of the most important lessons learned is that the end user or analyst must have software that is simple to learn and contains a minimum of "wizard-features". We believe that we must use the same technology and graphical user interface as the analysts share with their children and spouses at home. We learn by socialising with our friends and families.

If you are a cyber soldier or an information scout you are used to—and live in the rapidly changing software battleground.

However, for the analyst, the **need is not survival on the front line** but rather a calm and stable environment for analysing the information and producing intelligence. If you change the operating environment for the analyst too often, part of their days will be devoted to **taming the tool.**

Do not waste their time with unnecessary options and new versions of software until there is a real demand for new options.

As an example: One of the best analytical mind and graphical mind mapping tools we seen so far is Microsoft Encarta with the note an pushpin function. It is not big buck GIS software but it is cheap, easy to use and your children can help you if you get stuck!

Today we still use cheap off-the shelf software, simple and affordable servers and ordinary PC for the end user.

In our organisation we use effective, simple off the shelf tools that also are very inexpensive.

This means that we can afford to make mistakes, to change, to constantly do R&D in the area of text retrieval. If we invest in a high-tech million dollar system that works effectively today, we can not, due to budget restraints invest in next years wizard software.

In our Open Source-centre we take the most relevant and best information from INTERNET and from our other providers and sources -structure and it in a single document base that is accessible with one software tool. The analyst doesn't have to learn the continuously changing retrieval systems. What we do is to create one meta-provider with both an electronic and human interface.

This creates space and time for the analysts main mission. To create knowledge or intelligence out of the information we have collected and structured!

And we must remember one important truth.....

We are competing with the papers and specialists forum around the world. Our decision-makers read the newspapers watch the broadcasts from CNN etc.

We must digest more information in a shorter period of time; **we must reduce the time for transformation from information to intelligence.** The days of status quo are forever gone. And speaking about the media.....

Misinformation

One of the biggest keyword for NOT implementing OSINT in an intelligence process is MISINFORMATION. “The OSI is full of misinformation and attempts of deception”….??? Well that may be true. Nevertheless, it is in the same degree true for both SIGINT and HUMINT.

As an example:

Source A, belonging to a rouge diplomatic mission in one of the intelligence agency target countries, use the telephone frequently. In a conversion with Source A base at home Source A may be saying something like u I have information that the leaders of the subversive European Union have been here discussing R, S and T"

This conversion is intercepted by SIGINT and forwarded to the databank or the archives at the intelligence agency, The conversion is upgraded to state secrets because of the way of collecting not necessarily the content. HOWEVER, the analyst regards the SIGINT information as validated and VERY important.

The fact that SOURCE A may have heard about the meeting in the broadcast of the local radio or read The Economist and then talked about it a couple of days later NOT citing the original source is forgotten.

What do I mean? OSI may have the benefit of teaching cold war analysts and just out from the university the art of looking at every piece of information with the same critical eye regardless if its HUMINT, SIGINT or OSINT.

In my opinion the most valuable characteristic about OSI is

You always know the source, if it is primary or secondary
- It is cheap
- It is fast
- It is available

Some of the key lessons that we have learned are:

- Focus on finding quality primary sources.
- Keep all information in one format.
- Do it simple
- Maintain the human filter.
- Give the analyst only one - simple - tool

And most important of all

Sharing is Power!

OPTIMISING OPEN SOURCE INFORMATION SHARING IN AUSTRALIA: REPORT AND POLICY PRESCRIPTION – (Part IV, V)

Lieutenant Colonel Ian Wing - 1999
Chief of the Defence Force Scholarship Fellow
Australian Defence Force

Australia is taking positive steps to optimise open source information (OSI) and open source intelligence (OSINT).

Part Four: OPEN SOURCE SHARING IN AUSTRALIA

Current Australian Arrangements – National Security

The intelligence agencies involved in national security have made progress in the discipline of OSINT over the last few years. The scope and extent of this progress has varied from agency to agency.

DFAT

The Department of Foreign Affairs and Trade operates the Open Source Collection Unit (OSCU) which contributes to the Foreign Broadcast Information Service (FBIS).

Case Study – ASIO (1)

The Australian Security Intelligence Organisation draws heavily on open source capabilities.

ASIO has developed the Intelligence-Based Decision Model (IBDM) and it allows each element of the intelligence 'business cycle' to be identified and compartmentalised into workable projects within a strategic planning framework.

Intelligence is only one part of the general policy process and ASIO recognises that its clients receive advice from many other sources, which may differ from ASIO's advice. ASIO seeks to understand the whole decision-making process: the policy framework; the stakeholders and their expectations; the attitudes of clients; and the real or implied intentions of alternative advice. The intelligence adviser who fails to pay heed to open source material may find that their client has a better idea of the general situation and a set of predispositions that any amount of covertly-sourced material may be unable to shift.

OSI forms a key element of the 'all-source continuum' which has several broad characteristics relating to the utility or otherwise of OSI and Covert Source Intelligence (CSI):

Open Source Information	**Covert Source Information**
Open Access	Closed access
Cheap	Expensive

Reliability unknown	Reliability known
Independent	Dependent
Unstructured	Structured
Low risk	High Risk
Least Intrusive	Highly intrusive
Overt	Covert

In practice the all-source continuum includes three groupings of sources which have hazy boundaries. These are:

- open, publicly available information (such as the media, on-line sources and the Internet);
- restricted access (such as police information, official information and foreign government records); and
- closed and/or covert (such as national security information and protected sources).

ASIO applies a structured approach to security risk management using the Security Risk Matrix (SRM). The SRM consists of:

- Likelihood of Threat x Nature of Consequence = Risk
 - Intent x Capability = Likelihood of Threat
 - Desire x Confidence = Intent
 - Resources x Knowledge = Capability

The hypotheses used by ASIO in the SRM process are generated using OSI . The hypothesis is then tested with additional specific monitoring and limited investigation, and a requirement collection plan is developed. To complete the assessment it may be necessary to access all available sources of intelligence and maintain collection and assessment activity if the security environment is particularly volatile or uncertain.

The ASIO Library provides a significant OSI capability to the organisation. It cooperates closely with other OSI units within the Australian intelligence and law enforcement arenas.

Case Study – DIO (2)

DIO has been officially exploring the utility of open sources since 1995. DIO has an Open Source Unit (OSU) co-located with the Information Centre. The primary open source is the Internet, complemented by participation in the US Government sponsored Open Source Information Service (OSIS), and traditional hard copy library resources. In addition, it has continued to exchange material with FBIS. It receives direct syndicated media feeds, and the DIO 24 hour watch maintains continuous monitoring of the international electronic media.

Their Internet experience suggests that there is a huge and diverse quantity of material (much of it at little cost) but the more useful data-bases and services do require quite substantial subscriptions. A properly trained and equipped unit of specialists is considered more effective than providing Internet access to all-source analysts.

Foreign print media coverage remains limited by translation capacity, but this adds another dimension of support to analysts covering topical geographic issues and crises. Customers will often obtain news reports and they are at times inclined to act upon them. DIO has a particular responsibility to verify the reports and place them into context.

The Open Source Unit, and the 24 hour watch, understand both the intelligence process and current topics of interest. This enables them to add significantly to the all source analysts' work. All of this is being done with material that is significantly less expensive to obtain than that from the more traditional sources. This in turn allows the other collectors to focus their energies on doing things which only they can do - and obtaining information which is not available in the public domain. Indeed, open source material can help better to articulate the true intelligence gaps which Australian classified sources must fill.

The Australian Imagery Organisation, which was raised from within DIO last year, utilises open source commercially available imagery in conjunction with classified imagery and all source intelligence. It produces analytical support products, targeting material, contingency support packages and military mapping products.

A National Intelligence Principle (3)

An important principle relevant to the collection of information by the sources of the Australian intelligence community is that covert collectors do not target information if that information is available through other overt means. Besides the waste of agency resources by unnecessarily duplicating the work of each other, why incur the relatively higher cost of covert intelligence collection, and the associated political risk, if this too is not necessary?

An exception to this principle occurs when doubt exists about the accuracy of information received from overt sources. In such cases, covert intelligence might be sought to provide independent verification.

Current Australian Arrangements - Law Enforcement

In the law enforcement arena, OSINT is an important part of the operation of several federal and state level agencies and police forces.

Case Study – OSCA (4)

The Office of Strategic Crime Assessments observes trends in challenges to strategic law enforcement with significant input from its open source cell. OSCA has never run a 'traditional' in-house library service. Instead, it has access to, and support from, the libraries of the Australian Institute of Criminology, the AFP and the Attorney-General's Department . It uses in-house information professionals to provide dedicated support to its intelligence analysts by facilitating access to information and sources required for intelligence assessment work.

OSCA is tasked with analysing the entire criminal environment - and therefore has a very wide scope to its areas of intelligence interest and information requirements. To be able to put together a comprehensive view of the 'big picture', OSCA needs to be able to draw on a very wide information base for its knowledge of all issues of concern.

Every aspect of OSCA's information collection and management activities is carried out according to systematic, disciplined processes. Comprehensive strategies are devised for the ongoing development and operation of all information services. These are included in an Information Collection and Management Strategic Plan, produced approximately every 18 months. The primary operating principle is that all information - regardless of its source, format, or any other distinguishing feature - is collected and managed according to its value to the organisation.

OSI is essential to OSCA for monitoring the global strategic environment; for 'scanning the horizon' for emerging political, economic, social and technological trends and developments; and providing other general broad contextual information. OSI can provide early warning of emerging issues: by taking small, disparate pieces of information from many different sources (like news media, journals, web sites, etc) and pulling it all together to give a picture of the broader emerging strategic environment. OSI can also give OSCA 'rapid orientation' to new issues. OSCA uses a number of online services, including Reuters Business Briefing, FBIS Online, UnCover Reveal, DIALOG and LEXIS-NEXIS, and the Internet is used in a systematic manner.

OSCA likes to use OSI in its reporting. Where similar information is available from both open and official sources, the open source material will usually be cited. This assists in keeping the security classification of reports as low as possible - thereby facilitating wide dissemination - while at the same time protecting any sensitive intelligence sources and methods.

In 1997, OSCA built the Information Requirements and Intelligence System (IRIS), a Microsoft Access database that allows it to manage knowledge of all information requirements, information holdings, information sources and contacts, and other elements of the OSCA information environment in an integrated manner.

Case Study - CLEICC OSI-SIG (5)

OSCA also has a role in the coordination of the Commonwealth's law enforcement intelligence arrangements - primarily through its chairing of the Commonwealth Law Enforcement Intelligence Consultative Committee (CLEICC). The CLEICC recently established an Open Source Information Special Interest Group (OSI-SIG). With representation from intelligence and information professionals from across the law enforcement and intelligence communities, this group aims to facilitate:

- increased sharing of knowledge and experience of OSI-related issues;
- codification of 'best practice' in OSI activities, where appropriate;
- development of opportunities for cooperative and collaborative OSI activities; and
- the establishment of networks between officers in the community who develop and manage OSI collection and exploitation programs and activities.

The OSI-SIG has already identified an Internet exploitation strategy as one area which may benefit from collaboration. Such a strategy would primarily focus on the community-wide sharing of knowledge of valuable web sites and other Internet-based information resources.

Case Study – ABCI (6)

The Heads of Criminal Intelligence Agencies (HCIA) conference in September 1998 directed that the ABCI prepare a business case for the establishment of a centralised open source unit. This was announced by Paul Roger, Director of Intelligence of the Queensland Criminal Justice Commission, in his paper presented at 'Optimising Open Source Information'. (7)

The business case proposes that a small open source organisation be raised within the ABCI. It will be responsible to the HCIA and to an Open Source Intelligence Steering Committee.

The open source unit will meet Australian law enforcement requirements for collection and dissemination of open source material. The clients of the open source unit will initially be limited to the agencies that comprise the Criminal Intelligence Agencies. After the unit is established, additional agencies may be included as clients of the open source unit if a need is identified for using the service or on pay for service basis. Outsourcing open source collection to a commercial information broker is an option worthy of consideration.

The establishment of an open source unit provides the criminal intelligence community with an ideal opportunity to market an information brokerage service to other agencies. There is also the potential for the law enforcement unit to become part of a larger unit, and opportunities for networking between other OSI units including the RCMP, EUROPOL and the UK's Metropolitan Police.

The unit will initially concentrate on providing open source information rather than intelligence. When the unit has found its niche it can then concentrate on four other functions: current awareness briefs; rapid response to reference questions; contacting outside experts for primary research; and coordinating strategic forecasting projects. It will draw on the full range of external open sources, software and services.

The first consideration for implementing a centralised open source unit is determining a budget. Robert Steele has suggested that in the experience of the US intelligence community, no less than 1% of the total organisational budget is required. The detailed business case submission is currently being considered by the Federal Minister for Justice and Customs.

Case Study – New South Wales (NSW) Police Service (8)

The NSW Police Service recently established an OSI Unit to maximise the use of Internet within the Service. The unit evolved from a simple beginning, associated with the creation and maintenance of the 'Crime Stoppers' web site on the Internet, which was established in August 1996.

The OSI Unit has a dual role of supporting analysts in the production of strategic assessments as well as providing information relevant to the tactical and operational needs of front line police.

The Service is expanding its approach to 'intelligence driven policing'. Police at the local patrol level are required to demonstrate how their operations and response procedures are driven by intelligence. Commanders cannot rely solely on personal judgments and hunches about the nature of crime in their areas. Police in all operational commands must make decisions based on analysis of statistical crime data, research of patterns and trends,

demographic and census data, and reliable and credible intelligence reports. To respond to the complexities of the operating environment, police require high quality, relevant information. The electronic open source environment is helping to meet this need.

The State Intelligence Group is the central intelligence entity providing strategic and operational support for the NSW Police Service. Analysts use open source information to conduct research on specific areas of crime such as youth crime, transit related crime, counter terrorism and organised crime. Analysts access news services from Reuters and AAP, media feeds for newspaper, radio and television. The Internet also provides information vital to law enforcement strategic analysis, including government data sets and publications, academic and research papers, commercial information.

On another context, the Internet is being used to share crime information between jurisdictions and to establish contacts with counterparts in law enforcement and criminology departments. Unlike some other intelligence products, the majority of strategic criminal intelligence is unclassified. This enhances the value of the Internet for exchange of information between jurisdictions.

The NSW Police service is the lead agency for the security of the 2000 Olympic Games (ASIO is the lead federal agency) and OSI will enhance its capabilities to meet this important responsibility.

Part Five: POLICY PRESCRIPTION

A Way Ahead

OSINT has the potential to integrate the wealth of sources, software and services from the private sector, with the process of intelligence.

The agencies of the Australian Intelligence Community in their strategic plans and policy groups have identified the need for improvement in the coordination of OSINT. This has been reinforced by the Australian National Audit Office report into the Commonwealth Agencies' Security Preparations for the Sydney 2000 Olympic Games which stated that:

> The Olympics will present challenges to ASIO in drawing on new overseas sources for information. It will take time to learn what information is available and how to deal with unfamiliar targets. It is important that processes be developed to maximise the access to sources of material and to avoid duplication of requests by Australian agencies. Access to open source material (eg. Internet and the media) may also be used to supplement other intelligence material. However, overseas experience suggests that the use of open source material can be resource-intensive. ASIO should undertake a thorough assessment of the extent to which this option should be used.

All of the agencies can work together to provide a coordinated OSINT capability. This capability would draw on the strengths of each of the intelligence agencies and create synergies between them, noting that many working relationships and shared efforts already exist in areas such as libraries and information technology.

The synergistic approach to OSINT would be guided by existing national intelligence policy (in the foreign intelligence, security intelligence and law enforcement intelligence fields). It would also develop a system in which the OSINT capabilities of each agency are matched to

its specific needs and shared with other agencies, in accordance with government accountability policies.

A future vision for OSINT is that the proliferation of open source information will enable the creation of a 'virtual intelligence community' in which open information sharing and open source intelligence production is commonplace. The community will include and draw strength from public and private sector entities lying outside the traditional intelligence and law enforcement fields. This development will not replace more traditional covert forms of intelligence collection and production, but it will increase their efficiency.

A future centralised national OSINT capability was foreseen at 'Optimising Open Source Information'. Whilst delegates envisaged the great advantages of such an agency, it was considered such a step would be unlikely to eventuate in the near future without a lifting of the current budgetary and bureaucratic restraints. Instead, significant advantages are likely to be obtained through the establishment of a centralised coordination capability. This capability should be based on shared inputs from the intelligence agencies and a synergistic approach to employing their joint capabilities.

The study of OSINT would be advanced through an 'information audit' across the Australian intelligence arenas, to determine current and expected dependency on OSINT. This would provide a basis for information planning, recognising that significant cost savings may accrue from a strategic shift to OSINT. The results of the information audit could be compared to the OSS benchmarks to ascertain levels of best practice in the field. A whole-of-government Australian operational concept for OSINT and a virtual intelligence community could then be developed. This concept should draw on the experience of other nations in this field.

A future Australian OSINT conference should be convened with the aim of building on the results of the 'Optimising Open Source Information' conference. This future conference could receive official support from the Australian Intelligence Community and should take place in 1999 or 2000 at the latest. The conference could enable detailed discussion of OSINT and include closed sessions to consider the relationship of OSINT with classified sources.

Recommendations

As a result of the deliberations of the 'Optimising Open Source Information'conference it was recommended that:

- The utility of OSINT and its ramifications receive further and continuing examination within the national security, law enforcement and business intelligence communities, with a view to the development of a synergistic and coordinated OSINT capability.
- An 'information audit' be conducted across the Australian intelligence arenas which would determine current and expected dependency on OSINT and inform a whole-of-government operational OSINT concept.
- A future Australian conference on OSINT be convened in 1999 with official support from the Australian Intelligence Community.

Conclusion - Important Issues

This paper has described how Australia is taking positive steps to optimise OSI. Several important issues require further effort to achieve optimum solutions.

First, there is a need for greater awareness and understanding about OSI and OSINT. Some middle level managers remain resistant to the introduction of capabilities which do not possess the normal characteristics of intelligence systems: high cost, high technology and high levels of secrecy. This education and understanding is being provided by conferences, meetings with practitioners from other nations, and by the demonstrable successes being achieved by existing OSI units.

Second, there is a need for greater differentiation between the professions of 'information specialist' and 'information systems/information technology specialist'. The former were once known as 'librarians' and they are the experts at finding information. For this reason, they have the potential to become Australia's OSI specialists. The latter are experts at creating computer-based systems. For this reason they play the important role of facilitating OSI through the employment of technology, but they are not necessarily as well suited to becoming OSI specialists.

Third, the budgetary restraints which operate within the official domain in Australia tend to be resistant to the introduction of new capabilities. This resistance can be overcome if decision-makers are made aware that although OSI and OSINT are not free, they can offer real savings in *overall* organisation expenditure. They can also offer increased coverage of areas of intelligence interest.

And fourth, the stove-piping of intelligence into specific disciplines, based on collection methods or customers, needs to be transformed into a cooperative and multi-disciplinary approach. OSI is likely to provide the circuit-breaker which will facilitate this process. It offers the opportunity to enhance cooperation between agencies and improve overall analytical performance.

The opportunities provided by OSI and OSINT have been recognised by many people working in the Australian intelligence profession. I confidently predict that Australia will make further progress in this field. The experiences of other practitioners in the fields of OSI and OSINT, and particularly those attending this conference, will play an important part in optimising Australian open source information sharing.

References:

1. This section of the paper is derived from 'Open Source Information and the Intelligence Based Decision Model' which was presented by Jason Brown of ASIO, at 'Optimising Open Source Information' 1998.

2. This section of the paper is derived from 'Open Source Applications in Defence Intelligence' which was presented by Major General Bill Crews, Director DIO, at 'Optimising Open Source Information' 1998.

3. This section of the paper is derived from 'Does Covert Intelligence Have a Future?' which was presented by Ian Dudgen, a senior intelligence consultant, at 'Optimising Open Source Information' 1998.

4. This section of the paper is derived from 'When Too Much Information is Barely Enough: OSI and the Office of Strategic Crime Assessments' which was presented by Dr Grant Wardlaw, Director OSCA, at 'Optimising Open Source Information' 1998.

5. Ibid

6. This section of the paper has been developed from 'Business Case for a Centralised Open Source Information Unit', ABCI, 27 January 1999.

7. 'The Requirement for a Law Enforcement Open Source Unit', paper presented by Paul Roger, Director of Intelligence, Queensland Criminal Justice Commission, at 'Optimising Open Source Information' 1998.

8. This section of the paper is derived from 'OSI in a Law Enforcement Environment' which was presented by Nola Watson, Director State Intelligence Group, NSW Police Service, at 'Optimising Open Source Information' 1998.

OPEN SOURCE INTELLIGENCE
A 'FORCE MULTIPLIER'

Lt Cdr Prashant Bakshi, Indian Navy, Research Fellow IDSA, New Delhi
***The Tribune* (India), Online Edition June 24, 2001**

Intelligence agencies have for long relied on SIGINT (Signal Intelligence), HUMINT (Human Intelligence) and COMINT (Communication Intelligence) for their information-gathering requirements. In recent times, 'open sources' have evolved tremendously to the extent that they are seriously considered a source of intelligence, hence the term OSCINT (Open Source Intelligence).

This can be attributed mainly to the proliferation of information and communication technologies, especially the Internet. Information earlier considered as classified is now widely available — and that too at a mere click of the mouse. For instance, during the recent US-China spy plane debacle, one could effortlessly download satellite images of the EP-3 surveillance aircraft parked at the Lingshui military airfield from the Janes defence website (www.janes.com). Furthermore, one could also learn from the website about a recent upgradation, SSIP (Sensor System Improvement Program), carried out on the aircraft, making it the most sophisticated airborne electronic surveillance asset in the US Navy. With such easy access to vital information, intelligence agencies are slowly but surely accruing more importance to OSCINT.

So, what exactly does OSCINT mean? The US intelligence community has aptly defined the term:

> "By Open Source we refer to publicly available information appearing in print or electronic form. Open Source information may be transmitted through radio, television, and newspapers, or it may be distributed by commercial databases, electronic mail networks, or portable electronic media such as CD-ROMs. It may be disseminated to a broad public, as are the mass media, or to a more select audience, such as grey literature, which includes conference proceedings, company shareholder reports, and local telephone directories. Whatever form it takes, Open Source involves no information that is: classified at its origin; is subject to proprietary constraints (other than copyright); is the product of sensitive contacts with US or foreign persons; or is acquired through clandestine or covert means."

OSCINT, however, applies the same fundamentals of traditional intelligence — sifting and analysing information to metamorphose it into unclassified intelligence. Often, such intelligence proves highly invaluable when integrated and validated with other sources, and of course, it needs to be finally given the strategic perspective by experts in the related subject. The advantages of OSCINT are immense and, no wonder, countries like the USA, Israel, Sweden and South Africa have adapted well to this form of intelligence and refer to it as a 'force multiplier'.

The common perception that OSCINT is a recent phenomena centered around the Internet is not quite true. In fact, intelligence agencies have always acknowledged the potential of Open Source Information. Take the case of FAS (Federation of American Scientists), a privately funded organisation, which was originally founded in 1945 as the Federation of Atomic Scientists. Over a period of time, it has evolved into one of the most comprehensive resources for Open Source Intelligence — conducting analysis and doing advocacy on a wide range of issues, which include science and technology, national security, nuclear weapons, arms sales,

biological hazards and space policy. If you are searching for information on Pakistan's nuclear reactors or an update on the Chinese cruise missile programme, a visit to their website (www.fas.org) would in all certainty overwhelm you with the kind of information that is available.

Even during the height of the Cold War, some 20 per cent of the information collected by the Americans on the erstwhile Soviet Union came from open sources. A case in point is the Foreign Broadcast Information Service (FBIS), a US government office chartered to monitor foreign (non-US) open source information for use by the US Government.

The FBIS offers an extensive, in-depth collection of translations and transcriptions of Open Source Information from around the world on diverse topics that include military affairs, politics, environment, societal issues, economics, and science and technology.

Today, there is no dearth of OSCINT sources. While most of them (see table) can be accessed on the web, companies like Janes, apart from having an online presence, also publish periodical reports and reviews that are available on subscription. In fact, the Janes annual books on aircraft, ships and weapon systems are nothing short of defence encyclopaedias that are extremely popular in defence libraries all over the world.

Amongst recent OSCINT sources, Stratfor (Strategic Forecasting) and OSS (Open Source Solutions) deserve due mention. While Stratfor started off as a think-tank; it earned due recognition during the conflict between NATO and Yugoslavia with more than 2 million people visiting the Stratfor website. Based in Austin, it has an experienced staff who strive hard to combine intelligence analysis with the rigours of journalism. Subscribers to Stratfor have a host of options — daily global updates to monthly reports — to choose from, and more so at the convenience of receiving it on one's desktop computer as an e-mail.

The OSS, on the other hand, is one of the world's first information merchant banks' practicing information arbitrage and delivering Open Source Intelligence consulting and services. Interestingly, the 'OSS has a unique feature called MindLink that allows members to join discussion lists dedicated to intelligence related topics. It also provides access to over 5,000 pages of material and two publications, a monthly *OSS Notices* and, a quarterly *Global Intelligence Journal.*

In the Indian context, the concept of OSCINT is still evolving; there are a few defence-related websites — bharat-rakshak.com and stratmag.com — that have sufficient ground to cover and be in the same league as their western counterparts. However, there are some news services like POT (Public Opinion Trends Analyses and News Services) which cover various issues in South Asia and publish bulletins on a regular basis.

Surprisingly, one hears more about occurrences of corporate espionage than military espionage, which can be attributed to the cutthroat competition among business conglomerates. This has led to a spurt in companies dealing with business and economic intelligence.

Future indicators convey a vast potential for OSCINT. However, it is unlikely that it would ever replace traditional clandestine techniques — spies and satellites. Open Source has a distinct advantage, that it is always readily available, as in the case of the Gulf War wherein CNN newscasts were potentially more useful to the first US planes over Baghdad since

classified information did not reach on time. Technology is changing at an amazing pace and hopefully advances in artificial intelligence techniques and development of information agents or 'bots' might make sifting and analysing data simpler and less time consuming. Whatever form it may take, technology would always be the means to an end; and not the end in itself.

REFERENCES

COLLECTION AND USE OF OPEN-SOURCE INTELLIGENCE

Compiled by J. Ransom Clark, The Literature of Intelligence
http://intellit.muskingum.edu/

Aftergood, Steven. "Intelligence and the Open Source Challenge," *Secrecy News* (from the FAS Project on Government Secrecy), 2 May 2001.

According to the "Strategic Investment Plan for Intelligence Community Analysis," produced by the National Intelligence Production Board (NIPB), "[t]he NIPB has made the development of an Intelligence Community strategy for open source a top priority for investment and concerted action over the next few years." In addition, the Intelligence Community "also needs to exploit the Internet and other open media more effectively and efficiently."

Betts, Mitch. "Agents Spy Internet Data." *Computerworld* 28 (1 Aug. 1994): 1, 101.

Comments from Joseph Markowitz, "director of the CIA's Community Open Source Program Office," on Intelligence Community components hooking up to the Internet "to collect and share 'open-source,' or unclassified, information." On the use of open-source information generally, Markowitz states: "The creation of our office is a recognition that open sources are a valuable resource. As we draw back in some parts of the world, our office provides an information safety net."

Bowen, Wyn. "Open-Source Intel: A Valuable National Security Resource." *Jane's Intelligence Review*, 1 Nov. 1999.

This article first offers "definitions of open-source information (OSINF) and open-source intelligence (OSINT). This is followed by a consideration of the utility of open sources in terms of complementing classified information. The article then proceeds with a brief conceptual consideration of the key steps in setting up and operating an open-source collection system. Key issues and problems associated with open source collection are subsequently highlighted. Finally, to provide an idea of the availability and scope of open sources with relevance to national security, some examples related to monitoring proliferation threats are provided."

Clift, A. Denis. "National Security and National Competitiveness: Open Source Solutions." *American Intelligence Journal* 14, nos. 2 & 3 (Spring/Summer 1993): 25-28.

Chief of Staff, DIA, from July 1991.

Cote, Maureen. "Translation Error and Political Misinterpretation." *Studies in Intelligence* 27, no. 4 (Winter 1983): 11-19.

Dandar, Edward F., Jr.

1. "Open Source Info." *INSCOM Journal*, Jan.-Feb. 1997, 16ff. [http://www.vulcan.belvoir.army.mil/BackIssues/JanFeb97/janfebpage16.htm]

2. "Open Source Information Strategy."*INSCOM Journal*, May-Jun. 1997, 32ff.[http://www.vulcan.belvoir.army.mil/BackIssues/MayJun97/MayJunPage32.htm]

The main thrust of these two articles is articulated in the following excerpt: "Intelligence experts must continue exploring ... open source information acquisition and exploitation alternatives, such as the use of commercial vendors, universities and military reservists. The intelligence community should explore simultaneous employment of these resources. These external internal community assets are uniquely capable of handling the information explosion and support a number of intelligence community and military core business areas."

Clark comment: It is instructive that neither article mentions existing Intelligence Community resources for the acquisition and processing of open-source information. The suggestions for enhancing Community access to open sources clearly have been influenced by Robert D. Steele (see below) of Open Source Solutions, Inc., whose assistance is recognized at the conclusion of the second article. Although I have nothing but respect for Mr. Steele's entrepreneurial spirit and acumen, he is not the first person to discover the value of open-source material (the predecessor organization of the CIA's Foreign Broadcast Information Service predates World War II). Whether intelligence decisionmakers should move away from long-established and cost-effective governmental open-source collection and management resources toward private-sector-generated materials is worthy of some debate.

Friedman, Richard S. "Open Source Intelligence." *Parameters*, Summer 1998, 159-165. http://carlisle-www.army.mil/usawc/Parameters/98summer/sum- essa.htm.

Friedman's essay "explores the significance of a trend toward increased recognition of the role of open source information and discusses what this may mean for intelligence consumers at every level."

Gwynne, Sam C. "Spies Like Us: The Internet Is Changing the World's Most Dangerous Game." *Time*, 25 Jan. 1999, 48.

Clark comment: If you can get beyond the silly (and incorrect) title (there are plenty of games in which there have been more deaths than the spy business), this article is about the growth of the use of open-source intelligence in the business world.

"[T]he World Wide Web has given birth to a whole industry of point-and-click spying. The spooks call it 'open- source intelligence,' and as the Net grows, it is becoming increasingly influential.... Among the firms making the biggest splash in this new world is Stratfor, Inc., a private intelligence-analysis firm based in Austin, Texas. Stratfor makes money by selling the results of its sleuthing (covering nations from China to Chile) to corporations like energy-services firm McDermott International. Many of its predictions are available online at www.stratfor.com."

Holden-Rhodes, J.F.

1. *Sharing the Secrets: Open Source Intelligence and the War on Drugs.* Westport, CT: Praeger, 1997.

According to **Turner**, *IJI&C* 12.1, this work presents a brief, "useful[,] and instructive" critique of U.S. anti-drug policies and activities. However, the author "ultimately falls short" on

his promise to show how open-source intelligence can be made "a fundamental part of the drug war."

2. "Unlocking the Secrets: Open Source Intelligence in the War on Drugs." *American Intelligence Journal* 14, nos. 2 & 3 (Spring/Summer 1993): 67-71.

This is a succinct presentation of some of the thoughts that the author develops in his *Sharing the Secrets* (see above).

Hutchinson, Robert. "Rumor of War: An Information Vendor's View of the Provision of Open-Source Data in an Unstable World." *American Intelligence Journal* 14, nos. 2 & 3 (Spring/Summer 1993): 33-36.

Hutchinson is an editor of Jane's.

Loeb, Vernon. "Back Channels: The Intelligence Community -- Non-Secrets." *Washington Post*, 1 Feb. 2000, A13. [http://www.washingtonpost.com/]

According to Robert D. Steele, former CIA operations officer and chief executive of Open Source Solutions Inc., "three of the Pentagon's joint commands have appointed action officers to manage the collection of openly available, non-secret intelligence.

"'There is growing interest among the theater commanders-in-chief in operationally oriented open-source intelligence,'" Steele said. "'The continuing difficulties faced by the CINCs in obtaining timely intelligence, including commercial imagery, from the Beltway bureaucracies have led them to begin creating their own direct-access capabilities for open-source intelligence.'"

See Steele, Robert David, below.

Loeb, Vernon. "Spying Intelligence Data Can Be an Open-Book Test: Firm Finds a Market for Publicly Available Information." *Washington Post*, 22 Mar. 1999, A17.

Robert D. Steele, chief executive of Open Source Solutions Inc., in Fairfax, Virgina, "thinks there is one aspect of the intelligence game that he plays better than his former employer: gathering up publicly available information."

Steele and his partner, Mark Lowenthal, "don't contend that open sources can replace clandestine human and technical sources. But the intelligence agencies exhibit a bias for their own secrets, they say, and lack internal systems for fully mining business experts, academic authorities, scientific journals, foreign government reports and burgeoning commercial databases, not to mention the Internet."

See Steele, Robert David, and Lowenthal, Mark, below.

Lowenthal, Mark. "Open Source Intelligence: New Myths, New Realities." Available at: http://www.defensedaily.com/reports/osintmyths.htm. *Intelligencer* 10, no. 1 (Feb. 1999): 7-9.

This is an excellent analysis of the problems surrounding the collection and use of open-source intelligence in the information world of today.

The author argues that the Community Open Source Program Office (COSPO), "the IC's attempt to arrive at a more coherent approach to the open source issues, both technology and content," failed to achieve its mission. The reasons for that failure can be found an "in-grained" Intelligence Community "prejudice ... against open sources," and an overemphasis on "finding an ever elusive technology that would solve the open source problem of multiple and diverse sources."

McGill, G.M. (Mert) "OSCINT and the Private Information Sector." *International Journal of Intelligence and Counterintelligence* 7, no. 4 (Winter 1994): 435-443.

"The amount of information available electronically through open sources, information with countless intelligence applications, is staggering.... The

intelligence community must take advantage of every possible resource at its disposal, including the wide array of open source information that is readily available and relatively inexpensive." The author's primary suggestion is for the government to release information in "raw" form through a network like the Internet; private-sector information providers would, then, package or add value to this data.

Sigurdson, Jon, and Patricia Nelson. "Intelligence Gathering and Japan: The Elusive Role of Grey Intelligence." *International Journal of Intelligence and Counterintelligence* 5, no. 1 (Spring 1991): 17-34.

Steele, Robert David

Robert David Steele is a former intelligence officer and President of Open Source Solutions, Inc., who has established himself as the leader in developing and propagating "private enterprise intelligence." He argues essentially that U.S. intelligence reform is needed, that reform should seek to maximize the use of open-source intelligence, and that the private sector can meet a high percentage of U.S. open-source intelligence needs at a reduced cost to the U.S. Government.

Other articles by Steele can be found under the "Reform" heading and at the web site maintained by Open Source Solutions, Inc.: **http://www.oss.net/**.

See (above) Vernon Loeb, "Spying Intelligence Data Can Be an Open-Book Test: Firm Finds a Market for Publicly Available Information," *Washington Post*, 22 Mar. 1999, A17.

1. *On Intelligence: Spies and Secrecy in an Open World.* Fairfax, VA: AFCEA International Press, 2000.

From **"Publisher's Foreword"**: "[T]his compendium of material on understanding the power of open sources [is offered] in the hope it will help chart the new course -- a new model -- for the future of intelligence."

Clark comment: This work brings together many of the thoughts on the state of U.S. intelligence and proposals for reform that have animated Steele's activities for the past decade. The author's hypothetical Senate Bill S.2001 makes hamburger of many sacred cows, but Congress has refused to act on much less radical measures. A terminology quibble: While I fully understand the need for breaking old molds, the title Director-General (as in, Director-General of National Intelligence) sounds more French than American.

While acknowledging that the author and his views remain controversial, **Jonkers**, *AFIO WIN* 19-00, 12 May 2000, finds that Steele's book "contains ideas to which we should pay attention. His vision, leading up to the 'virtual intelligence community' is worth consideration."

Steele provides the following thoughts on his work: "With a foreword by Senator David L. Boren, sponsor of the 1992 intelligence reform legislation, and blurbs from Alvin Toffler, Bruce Sterling, former DDCI Dick Kerr, and flag officers from Russia, Germany and the United Kingdom, this book is unique in that it provides an itemized list of U.S. Intelligence

Community budget cuts totalling $11.6 billion dollars a year; and completely outlines 14 major new initiatives for restructuring, enhancing, and considerably expanding our concept of 'national intelligence'. With a 50-page annotated bibliography that integrates Silicon Valley, Internet, management, and hacking books with the more traditional literature; a 62-page index; and 30 pages of proposed legislation, the National Security Act of 2001, this is a reference work."

2. "The Importance of Open Source Intelligence to the Military." *International Journal of Intelligence and Counterintelligence* 8, no. 4 (Winter 1995): 457-470.

"In general terms, OSCINT has significant potential as a source of intelligence support for indications and warning, policy development, contingency planning, security assistance, weapons acquisition (design and countermeasures), joint and coalition operations, and tactical operations against new priorities such as proliferation. Finally, OSCINT is vital as a means of rapidly orienting a commander and serving as the foundation for collection management within the traditional intelligence disciplines." (p. 459)

3. "National Intelligence and Open Source: From School House to White House." *American Intelligence Journal* 14, nos. 2 & 3 (Spring/Summer 1993): 29-32.

4. "Private Enterprise Intelligence: Its Potential Contribution to National Security." *Intelligence and National Security* 10, no. 4 (Oct. 1995): 212-228.

"The aim of this essay is to explore the larger strategic context within which private enterprise intelligence can make a contribution to national security; to understand operational concepts from private enterprise intelligence which can and should be adopted by the traditional government intelligence services; and finally, to make an inventory of some of the specific private enterprise intelligence capabilities which can be used by the government to achieve both tactical results and sustained savings.... [I]t is clear that OSCINT can meet the vast majority of America's intelligence needed against the emerging threats, and that OSCINT must be foundation upon which we completely restructure our classified capabilities."

The paper from which this article is derived, given at a conference on "The Producer/Policy-Maker Relationship in a Changing World," 29 October 1994, in Ottawa, is available at: http://www.oss.net/Papers/training/Lesson001Handout1B.html.

5. "Open Source Intelligence: What Is It? Why Is It Important to the Military." *American Intelligence Journal* 17, no. 1/2 (1996): 35-41.

"At this time the U.S. military does not have timely broad access to a full range of open sources." (p. 39)

6. "Smart People, Stupid Bureaucracies: A Tough Love Look at U.S. Spies, Satellites, and Scholars." 21 Dec. 1999. http://www.oss.net/Papers/white/SmartPeople.doc.

"In a complex world where billions of people live on $1 a day and yet have access to radios and televisions that depict the USA as 'the enemy'... we need to be seriously concerned about both the lack of public understanding of national intel, and the relatively pedestrian level of discussion that is found in major media and 'think tank' outlets. This article ... seeks to outline several common misunderstandings, to summarize the findings of the [18-20 November 1999] conference led by President Bush, and to outline fourteen areas where substantial improvements are required if our national intelligence community is to be effective in protecting America in the 21st Century. I would emphasize my belief that a renaissance of our secret national intelligence is necessary, while also stressing that a revitalization of this essential national capability cannot take place in a vacuum -- we must do better at scholarship and must be much more effective and honest in our corporate communications pertaining to real world issues. More fundamentally, our people -- our public and our press -- must understand the great importance of our classified national intelligence community to national security, and must also understand the larger context within which this intelligence community contributes to the intelligence qua 'smarts' of the nation as a whole."

The slides and planned text of the original presentation of Steele's "fourteen areas where substantial improvements are required," made to a meeting of government and industry managers of intelligence on 16 September 1999, are available at http://www.oss.net/Papers/white/TOUGHLOVE.ppt. "A longer document with detailed evaluations and financial recommendations is available at http://www.oss.net/OSS21."

Studeman, William O. [ADM/USN] "Teaching the Giant to Dance: Contradictions and Opportunities in Open Source Information within the Intelligence Community." *American Intelligence Journal* 14, no. 2 & 3 (Spring/Summer 1993): 11-18.

Remarks made at Symposium on "National Security and National Competitiveness: Open Source Solutions," McLean, VA, December 1992.

U.S. Central Intelligence Agency. *Preparing U.S. Intelligence for the Information Age: Coping With the Information Overload*. Washington, DC: 1993.

Surveillant 3.2/3: "The Scientific and Technical Committee (STIC) Open-Source Subcommittee ... believes there is an urgent need to develop automated tools for coping with information overload. The report gives an awareness of the extent of the problem."

Wallner, Paul F. "Open Sources and the Intelligence Community: Myths and Realities." *American Intelligence Journal* 14, nos. 2 & 3 (Spring/Summer 1993): 19-24.

DIRECTORY OF RESOURCES

Excerpt from "Open Source Exploitation: A Guide For Intelligence Analysts", produced by Open Source Publishing Inc. (http://www.osint.org/) for the Joint Military Intelligence Training Center (JMITC)

A

Alexa – http://www.alexa.com/
Alexa is an interesting project that is attempting to archive the Web while at the same time providing a means for collaborative filtering. The Alexa software creates a toolbar at the base of your browser which gives you information about the site that you are visiting and a list of suggested Web sites on the same topic. The toolbar also allows the user to access the Alexa Web archive.

About.com – http://www.about.com/
This search engine/service uses volunteers who are screened by About.com to ensure their expertise in the topic area they edit. Each About.com "GuideSite" is devoted to a single topic, complete with site reviews, feature articles and discussion areas.

AltaVista – http://www.altavista.digital.com/
A very fast and popular search engine created by Digital Equipment Corporation. Both Web and Usenet newsgroup content can be searched. Because of the size of its index, you should learn the advanced-search syntax for this engine to generate only the results you seek. Instructions for search syntax can be found on Altavista's home page.

Analyst's Notebook – http://www.i2inc.com/
The Analyst's Notebook is data visualization software that assists analysts by
locating, interpreting and displaying complex information in easily understood chart form. The Analyst's Notebook provides: association (link analysis) charts, commodity flow charts and timelines.

B

Bigfoot – http://www.bigfoot.com/
This site is designed to help you find e-mail, telephone and physical addresses. By providing information such as first and last names and state of residence, you can often find an individual's contact information.

BotSpot – http://www.botspot.com/
A portal site dealing with information robots (frequently called "bots"), spiders, wanderers, etc. An excellent site for individuals who are interested in the application of artificial intelligence to the Internet.

BullsEye – http://www.intelliseek.com/
A software tool that scans the most popular search engines and delivers hit results and descriptions to the user. The results can be saved for future reference or review. BullsEye also allows you to track changes to a site and provides a workgroup compatible interface. See also Copernic, LexiBot, OS-Mosis, SearchPad and WebFerretPRO.

C

Copernic 2000 – http://www.copernic.com/
A free software tool that scans the most popular search engines and delivers hit results and descriptions to the user. The results can be saved for future reference or review. Copernic also searches Usenet groups and email directories. Enhanced Plus and Pro versions of Copernic are available for a fee. See also BullsEye, LexiBot, OS-Mosis, SearchPad and WebFerretPRO.

D

Deja.com – http://www.deja.com/
This search tool indexes the contents of the more than 20,000 Usenet newsgroups. It is the most complete index of these newsgroups. Now run by Google.

Dogpile – http://www.dogpile.com/
An excellent meta search engine that is sophisticated enough of to allow the user to enter limited Boolean operators.

E

EuroSeek – http://www.euroseek.net/
Europe's premier search engine that supports searches in 40 languages.

Excite – http://www.excite.com/
A search engine which indexes Web sites and Usenet newsgroups. Excite attempts to do some analysis of your query terms in an attempt to find relevant sites even if they do not contain the exact terms you enter. Excite also offers a free news profile delivery service based on user-supplied keywords.

F

FAST Search – http://www.alltheweb.com/
The FAST Search Engine (Fast Search and Transfer) was originally a research project of the Norwegian Institute of Technology. FAST also contains links to popular search queries such as FTP and MP3. This search engine's owners are attempting to index one billion Web pages within the coming year.

Foreign Military Studies Office – http://call.army.mil/call/fmso/fmso.htm
The Foreign Military Studies Office (FMSO) assesses regional military and security issues through open source media and direct engagement with foreign military and security specialists to advise Army leadership on issues of policy and planning critical to the US Army and the wider military community. FMSO and its top notch military experts provide the Intelligence Community and DoD with excellent open source reporting.

Four11 – http://www.four11.com/
This site is a search engine designed to find e-mail and physical mailing addresses. Four11 also provides a telephone number search capability.

G

Google – http://www.google.com/
Google uses a complicated mathematical analysis to return high-quality search results. This analysis allows Google to estimate the quality, or importance, of every Web page it returns.

H

Highway61 – http://www.highway61.com/
This meta search site passes your query to seven major search engines. The combined results are presented in a single window, ranked by the number of sites on which the term was found and the ranking provided by each search engine.

HotBot – http://www.hotbot.com/
A search engine which indexes both Web and Usenet newsgroup content. This site offers a wide range of powerful search options including searches by geographic region. Queries are constructed using a graphical interface.

I

infoGIST – http://www.infogist.com/
infoGIST offers a wide variety of software applications that provide enhanced search and retrieval capabilities for the Web, intranets, LANs, subscription services, and your computer.

Infoseek – http://www.infoseek.com/
A search engine which indexes Web sites and Usenet newsgroups. Company and e-mail address lookups are also supported. This engine provides a rich set of indexed databases for searching.

ISYS – http://www.isysdev.com/
A number of text indexing and Internet related software packages that provide a very user-friendly interface. Also sells software for digitizing hardcopy documents and "spiders" for indexing external/internal Web sites. ISYS also allows the user to publish to the Web via its own search engine or to a searchable CD-ROM. See also ZyImage.

L

LexiBot – http://www.lexibot.com/
A search tool that does an extensive search of the Internet by leveraging search engines and Web databases. LexiBot uses a multi-threaded design, allowing it to make dozens of queries simultaneously. Documents are retrieved and prioritized for each search result. A free 30-day trial version of the software is available for downloading. See also BullsEye, Copernic, OS-Mosis, SeachPad and WebFerretPRO.

Lycos – http://www.lycos.com/
Lycos is a powerful search engine that indexes Web content. Lycos is very fast and has a number of useful features to help refine a user's search.

M

MetaCrawler – http://www.metacrawler.com/

This meta search site searches nine different search engines. Query results are returned ranked by relevance on a single screen.

Microsoft Internet Explorer – http://www.microsoft.com/
One of the two most popular World Wide Web browsers that are available free for personal use. See also the Netscape listing.

MSN Web Search - http://search.msn.com/
A popular Internet search engine that has an excellent help section.

N

NBCi – http://www.nbci.com/
A relatively new portal that includes a search engine formerly known as Snap.
Snap is a search engine that features content from over 100 leading Web publishers. The heart of NBCi portal services is a directory of Web sites and over 500 resource centers, built by a team of editors and reviewers.

Netscape – http://www.netscape.com/
One of the two most popular World Wide Web browsers that are available free for personal use. See also the Microsoft Internet Explorer listing.

Northern Light – http://www.northernlight.com/
Currently the largest of the Web search engines. Search results are combined with Northern Light's Special Collection documents that comprise 5,400 full text information sources. Access to the Special Collection documents requires a credit card.

O

Open Directory Project – http://www.dmoz.org/
A search engine/service that emulates the Yahoo! concept of categorization. The Open Directory Project uses volunteers to provide the bulk of the Web categorization functions. Search engines like Lycos and Hotbot also utilize Open Directory Project's categorization.

OS-Mosis – http://www.os-mosis.com/
An excellent Web search tool that allows the user to create and populate a database using a simple floating toolbar. The toolbar allows the user to capture and categorize information from a Web browser or word processor. Users are able to capture images, create categories and automatically acquire URLs and individual Web pages. OS-Mosis then creates a Web site from the user's database in a number of different layouts and configurations. A multi-user version is now available to help organizations manage their open source acquisition efforts. See also BullsEye, Copernic, LexiBot, SeachPad and WebFerretPRO.

P

ProFusion – http://www.profusion.com/
Profusion was recently purchased by Intelliseek the makers of BullsEye. ProFusion is a meta-search engine allowing you to query numerous search engines simultaneously. It also allows you to save your searches for later retrieval.

S

Search Engine Watch – http://www.searchenginewatch.com/
A Web portal dedicated to information about search engines. If you're interested in keeping track of the ever-changing world of search engines, this site is among the most complete of resources on the topic.

Search Engines Worldwide – http://www.twics.com/~takakuwa/search/search.html
Search Engines Worldwide provides an exhaustive listing foreign search engines organized by country or region. As US based search engines rarely index foreign language Web pages, this is an excellent resource.

Subject Search Spider (SSSpider) – http://www.kryltech.com/
Subject Search Spider is software that allows you search the Web by querying dozens of search engines simultaneously. Results are displayed through relevance ranking with duplicate Web sites automatically removed. You can also store your searches locally for later viewing.

SYSTRAN – http://www.systransoft.com/
The SYSTRAN site offers free access to its machine translation software that automatically translates text or entire Web pages from French, German, Italian, Portuguese and Spanish into English. It can also translate from English into the aforementioned languages. Far from a perfect translation, SYSTRAN does provide a good enough translation to enable the user to get the gist of the article or text.

T

Teleport Pro – http://www.tenmax.com/
One of the better off-line browsers that allows you to duplicate Web site data for fast offline access.

U

Usenet Groups
Usenet groups are electronic discussion lists similar to electronic bulletin boards. Users subscribe to a Usenet group to engage in or read about a discussion with other users. Each Usenet group is focused on a particular topic be that politics, medicine, religion, current events, etc. For search engines that index Usenet groups see also the Deja.com and Altavista listings.

W

WebFerretPRO – http://www.ferretsoft.com/
A software tool that scans approximately 30 search engines and delivers hit results and descriptions to the user. The results can be saved for future reference or review. The Power User Pack also searches Usenet groups, current news, e-mail addresses and telephone listings. See also BullsEye, Copernic, OS-Mosis and SearchPad.

Wisdom Builder – http://www.wisdombuilder.com/

A text indexing/link analysis/data visualization tool that allows you manage and manipulate large volumes of data. Wisdom Builder also markets its Gold Rush search software that is an artificial intelligence-based meta "find" engine that focuses on extremely high quality search results in a natural language processing based search environment. A free 30 day trial version of Gold Rush is available for downloading.

Y

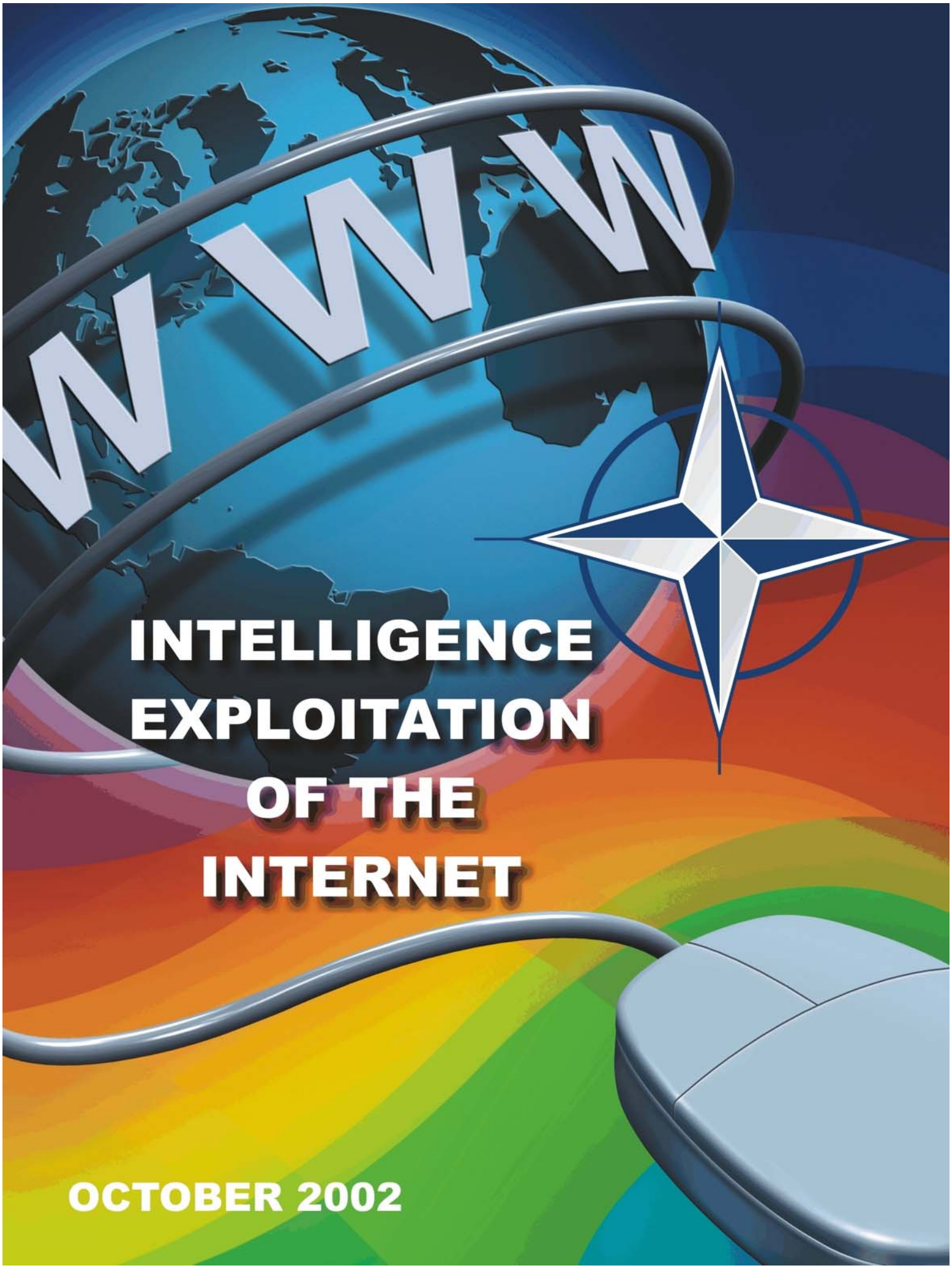
Yahoo – http://yahoo.com/

This service provides a directory of sites screened by staff reviewers. It is an excellent place to start a search, although does not add new Web sites as frequently as most other search engines. If the Yahoo directories do not provide relevant sites, you will be referred to other search engines.

Z

ZyImage – http://www.zylab.com/

An excellent text indexing, archival and dissemination software package that allows the user to digitize large volumes of paper documents or electronic files. ZyImage also allows the user to publish to the Web via its own search engine or to a searchable CD-ROM. See also ISYS.



INTELLIGENCE EXPLOITATION OF THE INTERNET

OCTOBER 2002

TABLE OF CONTENTS

INTRODUCTION **4**

CHAPTER I: INTERNET OVERVIEW **6**

Section A: World-Wide-Web (WWW) **6**

Section B: Newsgroups **8**

Section C: Email List Overview **11**

Section D: Chat **13**

CHAPTER II: DIRECTION **14**

Section A: Mission Analysis **14**

Steps in Mission Analysis 14
Step 1: Sources of the Mission 15
Step 2: Superior's Mission and Intent 15
Step 3: Derive Elements of Own Mission 17
Step 4: Identify Assumptions 17
Step 5: Identify Objectives 18

Section B: Primary Intelligence Requirement (PIR) Development **18**

Direction Development Worksheet 19

CHAPTER III: COLLECTION **20**

Section A: Collection Planning **20**

Collection Management 20
Making a Collection Plan 20
An Internet Collection Plan 21
The Internet Collection Planning Steps 22
Step 1: Determine Searchable Information Requirements 22
Step 2: Determine Best Site or Search 22
Step 3: Identify the Details to Access or Find Specific Information 22
Step 4: Determine Search Time Constraints 23
Using the Internet Collection Plan 23
Standing Requirements 23
Internet Collection Plan 24

Section B: Search Strategies **25**

Search Methodology 25
Prepare Before You Search 25
Step 1: Identify Key Concepts 25

Step 2: Identify Possible Search Terms 26
Topic Development Worksheet 26
Step 3: Decide Which Method to Use To Search 28
Step 4: Construct Your Search 31
Step 5. Limit Your Search 36
Step 6. Refine Your Search 37

Section C: Search Worksheet 39

Section D: Search Tools 41

Search Engines 41
What are search engines? 41
How do search engines work? 41
What are the pros and cons of search engines? 42
Are search engines all the same? 42
How do search engines rank web pages? 42
When do you use search engines? 42
Major Search Engine – Features Guide - 2002 46
Search Tools 50
Copernic 50
Deep-Web/Invisible Web 50
Searching the Invisible Web 50
Deep Query Manager 51

Section E: Searching Anonymously On The Web 53

CHAPTER IV: PROCESSING 56

Section A: Source Evaluation 56

Critically Analysing Information Sources 56
Determining the Source of Web Pages 59
Step 1: Study the URL 59
Step 2: Do a "whois" on the domain name 59
Step 3: Perform a Traceroute to the host name 61
Step 4: Read the web-page and follow-up with the point of contact (if any) 61
How to Read a URL 62
Traceroute 63
McAfee Visual Trace 66

Section B: Evaluation Checklists 68

Evaluation Checklist for an Advocacy Web Page 69
Evaluation Checklist for a Business/Marketing Web Page 70
Evaluation Checklist for a News Web Page 71
Evaluation Checklist for an Informational Web Page 72
Evaluation Checklist for a Personal Web Page 73

Section C: Validated Source Lists 74

Powermarks 3.5 74

Section D: Effective Summary **77**
Copernic Summarizer 77
CHAPTER V: DISSEMINATION **79**
Section A: Report Layering **79**
Section B: Dissemination with *Microsoft Outlook* **80**
Section C: Dissemination and Classification **82**
ANNEXES: **84**
Annex A: More information on Source Evaluation **84**
Searching Upstream 85
Annex B: Selected Information Sources **88**
a. Terrorist Threat Research (Rev 04 Mar 02) 89
b. Hostile Intelligence Threat Research (15 Feb 02) 93
c. Criminal Threat Research (15 Feb 02) 96
d. Medical Threat (Rev 08 May 02) 98
e. Geo-Political, Military & Country Information Research (Rev 04 Mar 02) 99
f. Geo-Political & Military Information – Russian Annex (Rev 04 Mar 02) 101
g. Gazetter, Port, Geodessy and Map Research (Rev 02 May 02) 102

INTRODUCTION

This handbook is the third in a series of publications produced by SACLANT to improve the understanding of Open Source Intelligence (OSINT) within NATO. The first publication, the NATO OSINT Handbook served as an introduction to the field of OSINT. The second volume, the NATO OSINT Reader was intended to provide under one cover a collection in international writings on the uses of open information sources in the preparation of intelligence products.

This volume is entitled Intelligence Exploitation of the Internet. In contrast to the first two volumes, this publication is intended primarily as a practical guide to the exploitation of an information source. While many people wrongly equate the Internet with the totality of open sources, it does currently serve as an important information source for many intelligence staffs. Although much information is available on the Internet, the Internet is in reality a communications medium upon which information flows rather than an information repository in its own right.

The Internet has largely replaced dedicated stand-alone communications networks used by commercial information providers to distribute their products. Specialized information such as ship and aircraft movement data, along with virtually all commercially published material can be accessed via the Internet through commercial information vendors. These sources often provide the most valuable unclassified intelligence data. The use of data distribution services such as FACTIVA, LEXIS-NEXUS or DIALOG requires specialized training to match sources to information requirements and thus remains outside the scope of this publication.

Rather, the aim of this publication is to expose intelligence staffs to many of the challenges of using information found via the Internet for intelligence purposes. It is structured according to the intelligence cycle.

CHAPTER II: DIRECTION underscores the importance of ensuring that information needs stem from mission requirements. The process of conducting mission analysis leading to the preparation of Primary Intelligence Requirements is explained.

CHAPTER III: COLLECTION begins with the process of preparing a collection plan using Internet sources. It continues with an examination of search strategies and tools. It concludes with a short discussion of the dangers associated with exposing intelligence interests through the trail that an Internet search leaves on the Internet.

CHAPTER IV: PROCESSING focuses on how to shape information gathered from the Internet, adding analysis, into intelligence – information that is relevant, reliable and that contributes to the generation of knowledge. It begins with how to analyse the source of the information. While classified intelligence collection disciplines typically discriminate between evaluated and unevaluated information, all data gathered from the Internet must initially be treated as unevaluated. It is through the process of source evaluation by an

analyst that information can be given greater credence. The Processing Chapter concludes with descriptions of tools that aid in the maintenance of validated sources and the importance of reducing information overload.

This volume concludes with CHAPTER V: DISSEMINATION. This chapter outlines a number of dissemination advantages that arise through the production of intelligence from unclassified sources. In particular, the advantages of using open sources to support the production of intelligence for coalition operations are explained.

The annexes include additional amplifying material. Annex A: More information on Source Evaluation provides some additional techniques to use in the evaluation of information sources prior to accepting information contained within their web-pages. Annex B: Selected Information Sources was developed by CINCEASTLANT Intelligence Staff and contains practical search tips, techniques and sources for Internet research on a number of relevant NATO intelligence topics of interest.

Much of the information contained in this volume has been copied directly from Internet sources. Rather than try to replicate many of the excellent training sources already in existence, this volume gathers together a number of relevant published writings. The source has been cited wherever possible. Care has been taken to organize the resulting collection into a user-friendly format. Additional topics have been addressed with original material so as to ensure that this volume comprises a complete introduction to intelligence exploitation of the Internet.

CHAPTER I: INTERNET OVERVIEW

Section A: World-Wide-Web (WWW)

1. What is the Internet?

The Internet is a network of networks, linking computers to computers sharing the TCP/IP protocols[1]. Each runs software to provide or "serve" information and/or to access and view information. The Internet is the transport vehicle for the information stored in files or documents on another computer. It can be compared to an international communications utility servicing computers. It is sometimes compared to a giant international plumbing system. The Internet itself does not contain information. It is a slight misstatement to say a "document was found *on* the Internet." It would be more correct to say it was found *through* or *using* the Internet. What it was found in (or on) is one of the computers linked to the Internet.

Computers on the Internet may use one or all of the following Internet services:

- Electronic mail (e-mail). Permits you to send and receive mail. Provides access to discussion groups often called Listservs® after the software they operate under.
- Telnet or remote login. Permits your computer to log onto another computer and use it as if you were there.
- FTP or File Transfer Protocol. Allows your computer to rapidly retrieve complex files intact from a remote computer and view or save them on your computer.
- Gopher. An early, text-only method for accessing Internet documents. Gopher has been almost entirely subsumed in the World Wide Web, but you may still find gopher documents linked to web pages.
- The world wide web (WWW or "the web"). The largest, fastest growing activity on the Internet.

2. What is the World Wide Web and what makes it work?

The WWW incorporates all of the Internet services above and much more. You can retrieve documents, view images, animation, video, listen to sound files, speak and hear voice, and view programs that run on practically any software in the world, providing your computer has the hardware and software to do these things.

[1] TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

When you log onto the Internet using Netscape or Microsoft's Internet Explorer or some other browser, you are viewing documents on the World Wide Web. The current foundation on which the WWW is based is the programming language called HTML. It is HTML and other programming imbedded within HTML that make possible Hypertext. Hypertext is the ability to have web pages containing links, which are areas in a page or buttons or graphics on which you can click your mouse button to retrieve another document into your computer. This "clickability" using Hypertext links is the feature that is unique and revolutionary about the web.

How do Hypertext links work? Every document, file, site, movie, sound-file or anything you find on the web has a unique URL (Uniform Resource Locator) that identifies what computer the item is on, where it is within that computer, and its specific file name. Every Hypertext link on every web page in the world contains one of the URLs. When you click on a link of any kind on a web page, you send a request to retrieve the unique document on some computer in the world that is uniquely identified by that URL. URLs are like addresses of web pages. A whole cluster of internationally accepted standards (such as TCP/IP and HTML) make possible this global information retrieval phenomenon that transcends all political and language boundaries.

3. What is a Browser?

A browser is a program that resides on your computer enabling you to view WWW documents and access the Internet taking advantage of text formatting, hypertext links, images, sounds, motion, and other features. Netscape and Internet Explorer are currently the leading "graphical browsers" in the world (meaning they facilitate the viewing of graphics such as images, video and more). There are other browsers (e.g., Macweb, Opera). Most offer many of the same features and can be successfully used to retrieve documents and activate many kinds of programs.

Browsers all rely on "plug-ins" to handle the “fancier” files you find on the web. Plug-ins are sub-programs stored within a browser or elsewhere in your computer especially to support special types of files you may click on. If you click on a link, and your computer does not currently have the plug-in needed for the file you clicked on, you are usually prompted with an opportunity to get the plug-in. Most plug-ins are free, and easy and safe to install on your computer; follow the instructions you are given.

The main way in which browsers differ is in the convenience features they offer for navigating and managing the web and all the URLs you may want to keep track of. Netscape and Internet Explorer both offer the ability to e-mail documents, download them to diskette, print them, and keep track of where you've been and sites you want to "bookmark."

Section B: Newsgroups

There are over 60,000 Usenet newsgroups where Internet users exchange messages on specific subjects. If you can't find something online via search tools, then try the newsgroups. A fellow Internet user can probably lead you to the right information.

Main points:

- Usenet Newsgroups are a globally shared/distributed set of online forums where users can post messages to each other.
- Newsgroups can be subject oriented (alt.news.macedonia) or created based on geography (soc.culture.afghanistan).
- Newsgroups are not chat rooms. Chat rooms are a more real-time event, where the text of messages is displayed back and forth between users in near real time. Newsgroup postings are more similar to email messages that are posted into a shared area, where other users may reply back to the message over the next several days.
- Quality of content in a specific newsgroup depends on the culture of that newsgroups' following. This is an online city of over 100 million strangers.
- Take the time to watch and learn the culture of a group before participating (called lurking).
- Thou Shall **not** SPAM[2] the Internet!!!
- Recommended Newsgroup reader software is Forte Agent.

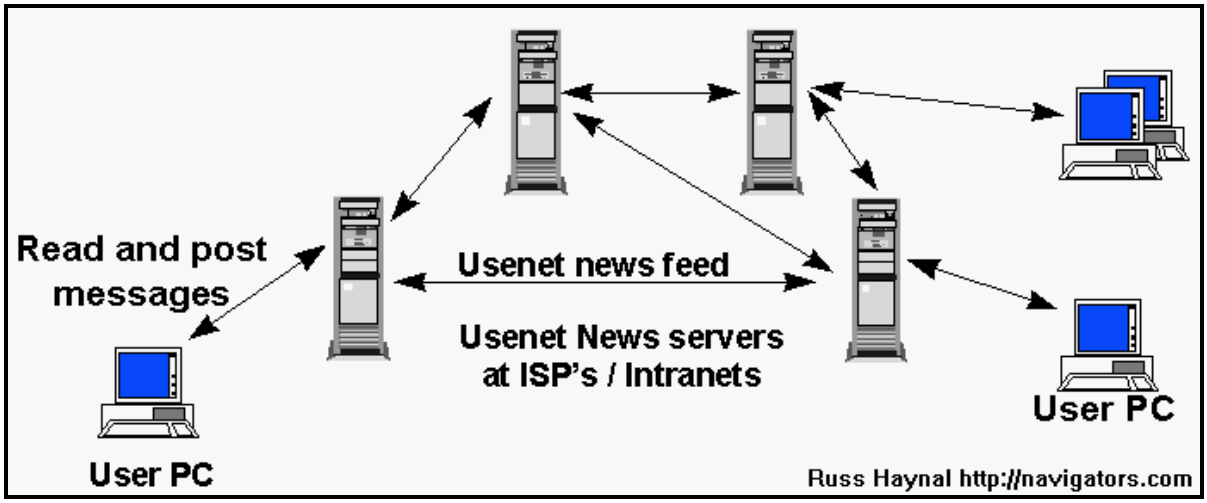
2 What is SPAM?

Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or quasi-legal services. Spam costs the sender very little to send -- most of the costs are paid for by the recipient or the carriers rather than by the sender.



- Messages (articles) are "posted" to the newsgroup
- Others may post their "follow-up" to the newsgroup OR may respond directly to the author via email
- A series of related "articles" is called a "thread"
- A FAQ (Frequently Asked Questions) may be posted. READ IT, to understand the purpose of the group, and to see if "your" question" is already answered in the FAQ. A list of FAQs is also available via the web.

Usenet Newsgroup Architecture



- Newsgroups are hosted on news servers throughout the Internet.
 - News Server onsite (i.e. news.company.com)

 - Use provider's server (i.e. news.ISP.net)

- Your local Newsreader is used to interact with this information. This can be a stand-alone Newsreader, or your web browser may also provide this capability. Check with your local Internet provider or network administrator for the software settings.
- You read and post messages to a specific new server. New postings are then fed to other new servers throughout the Internet, until each news server has a roughly equivalent set of messages.
- There are also public web-based news servers such as Dejanews which can be used by anyone.

Searching: There are several places on the Internet where the content of the newsgroups are being archived and made available for full-text searching: Dejanews, remarq, Altavista Usenet search, Liszt, tile.net. Google Groups.

For More Information:

- Usenet Topology -shows a small portion of usenet topology (in Italy)
- Top 1000 Usenet Sites - Shows which news servers are widely propagated.
- Emily Post News - great examples of what **not** to do in a newsgroups - a must read.
- Usenet death Penalty - See how the community can go after ISP's who permit Spam Abuse.
- Free advice on Usenet news - a fairly complete overview.
- NNQLINKS - news.newuser.questions contains a useful collection of information.
- Creating New Newsgroup - explains the process very well.
- Usenet Newsfeeds via satellite: Cidera, ispsat.

Source: http://navigators.com/usenet.html

Section C: Email List Overview

There are over 100,000 email lists where communities of Internet users share information and advice with each other.

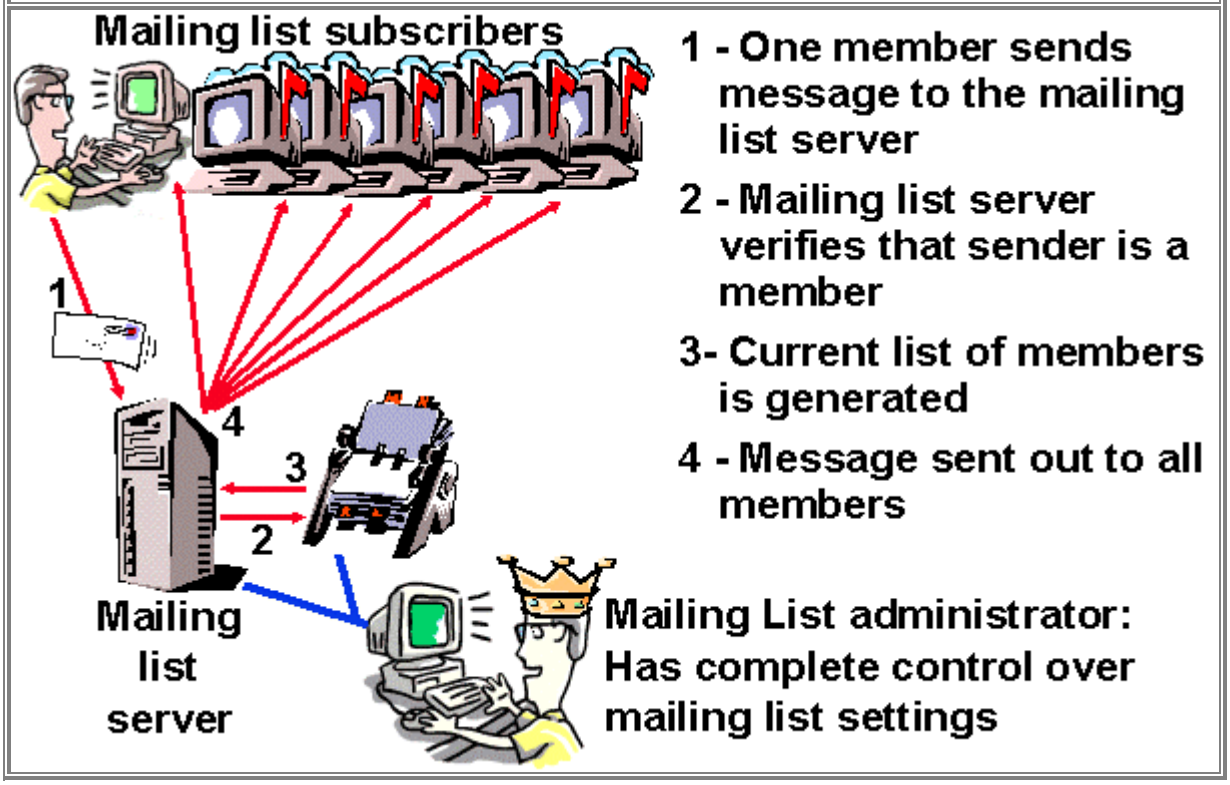
Main points:

- A mailing list provides an easy way for a large group of people to have an ongoing discussion via email.
- Most mailing lists are subject oriented.
- "Someone" must establish the mailing list and have it "hosted" at some list server. The "creator" of the mailing list is usually referred to as the list administrator.
- Mailing list software is often used to automate many of the list's functions such as joining a list and relaying emails to all list members.
- The mailing list will have an email address such as topic_name@hosting-site.com.
- Users must then **subscribe** to the list in order to receive the content of the mailing list. Subscribing is often done via an email command sent to the list_server [see above] software. For example:

To: listserv @ hosting-site.com from: your_email @ your-site.com subject: (you can leave this blank) subscribe topic-name

- As you subscribe, the very first message you receive will probably be a canned welcome message that the list_server send to all new subscribers. **Save** this welcome message. This message tells you what is the purpose of the list, what's allowed to be posted to the list, and most importantly, how to unsubscribe when you want to leave.
- At this point you might also begin receiving a flood of frequent email depending on the volume of the email list. You should definitely make a filter rule in **your** email client to handle all this new email.
- It is suggested that you "listen to the list for a while, before you jump in and participate (this is called "lurking").
- Some lists will allow any member to send a message to the rest of the group (Discussion-style) On other mailing lists, the mail administrator may be the only person allowed to post messages, much like a newsletter broadcast (announcement-style).

Sending an email to a mailing list



- Businesses can use mailing lists as a way to make announcements, send newsletters, or host product discussion groups.
- Mailing lists are especially useful for timely information and distributing information to a large number of people.
- Mailing lists can have some of the best information about a topic, because all the participants have made a commitment to receive all the messages being posted to the list. Unlike the newsgroups, something can be done about individuals who are abusing the groups' discussion. If enough people complain, the all-powerful list administrator has the ability to remove any individual who is not welcome on the list anymore.
- Searching for a mailing list? try PAML, CATALIST, TOPICA Meta-list.

For more information see:

- Email list software vendors: listserv, majordomo.
- Listserv top 20 - A daily indication of the largest mailing Listservs.
- Internet mailing list providers - this is useful for anyone who would like to create an email list.

Source: http://navigators.com/email_lists.html

Section D: Chat

Unlike the other communications venues described so far, chat rooms are synchronous. The conversations occur in real time, just like a conference telephone call. Chat rooms are typically found on specially programmed web pages. You type a message on the chat room screen and all the other people in the chat room see your name (or 'handle') followed by the message you are typing.

The best thing about chat rooms is that the communication back and forth is immediate. The conversation moves along as fast as the participants can read the messages and type in their replies. The disadvantages are that having more than 5-10 people in the chat room makes it difficult to follow the conversation because new messages are appearing on the screen before you have finished typing in your reply to a previous one. When your reply shows up on everyone else's screen, they may not know exactly what message your reply referred to.

The fact that everyone has to be there at the same time is also a disadvantage. The use of Chat Rooms for intelligence purposes begins to cross the threshold between OSINT (primarily passive) and HUMINT (primarily active collection).

CHAPTER II: DIRECTION

Section A: Mission Analysis

The classified intelligence production process within virtually all NATO Commands and member countries provides a stream of intelligence products. These are tailored to the intelligence needs of the recipient staffs based on established requirements. Access to a robust collection of open sources enables intelligence staffs to gather and process relevant information to supplement classified intelligence products. However, it provides much extraneous information as well.

It is folly to attempt to replicate on classified systems the host of relevant, reliable knowledge available from open sources. It is equally unwise to merely attempt to find information that may be relevant to a decision-maker on a topic that appears of interest. All efforts to effectively exploit any open source of information must be guided by mission requirements. Relevance is the key. Effective open source exploitation requires appropriate selection of sources and information.

"Relevance" judgments typically stem from the commander's Priority Intelligence Requirements (PIRs), which outline that intelligence deemed necessary by him to accomplish his mission. While ideally intelligence requirements should come directly from the commander, in reality, it is up to his intelligence staff to draft them based on an understanding of his intelligence needs. This process begins with mission analysis.

Within a staff structure, each staff element responsible to support the planning function with the development of estimates begins their work with their own mission analysis. As the intelligence staff is expected to provide the foundation knowledge upon which other planning is to be conducted, effective mission analysis is essential to generate appropriate intelligence products. Once mission analysis is complete, PIRs can be developed to support the mission needs. These PIRs in turn form the outline of collection plans where open sources are able to contribute alongside other intelligence sources.

Steps in Mission Analysis

Mission analysis is a part of the problem-solving technique that military staffs use to study a mission and to identify all tasks necessary to accomplish the mission. The process is as applicable to developing PIRs in advance of a military operation as it is in developing an intelligence production plan to support situational awareness. Mission analysis produces an understanding of the commander's information requirements based on an appreciation of the commander's responsibilities and those of his superior commander. Mission analysis is the primary factor in the development of an estimate. It

is also the initial step in understanding the relevance of an issue to a particular decision-maker (e.g. The threat of a South Asian war to a NATO commander) and those component elements of the issue that affect his mission (e.g. Danger of escalation/Impact on allied operations in theatre/etc).

When a commander receives a mission tasking, normally as a Warning Order, analysis begins with the following questions:

- What tasks must my command do for the mission to be accomplished?
- What is the purpose of the mission received?
- What limitations have been placed on my own forces' actions?

Once these questions have been answered, the commander can thoroughly understand the mission. When conducting OSINT exploitation in support of situational awareness, a similar set of questions emerge:

- How is this event relevant to my commander?
- What impact does this event have on assigned forces or potential operations?
- Will this event shift the operating environment within his Area of Operations?

Mission analysis steps relevant to the development of PIRs normally are as follows:

- Determine the source(s) of the mission.
- State superior's mission and intent.
- Derive elements of own mission.
- Identify (planning) assumptions.
- Identify objective(s).

Step 1: Sources of the Mission

One's own mission is typically a sub-set of the superior's mission. It is normally contained in the superior's directive either outlined specifically for a particular operation or more generally in guidance issued to subordinate commands. Intelligence staffs supporting situational awareness within a Strategic Command can derive mission sources from the NATO Strategic Concept, Command Strategic Guidance documents, political guidance issued from the North Atlantic Council (NAC) and military guidance issued from the Military Committee (MC).

Step 2: Superior's Mission and Intent

The initial concern during mission analysis is to study the superior's mission and intent. The latter is a concise expression of the purpose of the force's activities, the desired results, and how actions will progress towards that end. The commander's intent is not a

restatement of the superior commander's concept of operations, but is rather a description of what conditions – hostile and friendly – should result from the intended operations.

Normally the content of tactical, operational, and strategic commander's intent statements will be different, but the purpose will be the same: to provide guidance concerning the military/strategic "landscape" or the situation the commander wants to exist after the assigned military mission is accomplished. In general, the higher a command echelon is, the more likely that the commander's intent will be provided in writing or in message format.

An effective technique to evaluate the superior's intent is to practice the analytical technique of "problem restatement." How you define a problem determines how you analyse it. Through the following five step process, an analyst is able to better focus on the true issue rather than the problem that was initially presented.

Steps in Problem Restatement

1. **Paraphrase: Restate the problem using different words without losing the original meaning.** Trying to say the same thing with different words puts a slightly different spin on the meaning, which triggers new perspectives and informative insights.

2. **180 Degrees: Turn the problem on its head.** Taking the opposite view not only challenges the problem's underlying premises but also directly identifies what is causing the problem.

3. **Broaden the focus: Restate the problem in a larger context.** Look at the implications of the initial problem beyond the confines of your own organization.

4. **Redirect the focus: Boldly, consciously change the focus.** Using creative thinking, look at the problem from an entirely different perspective. (e.g. from "How do we defeat the insurgents?" to "How do we eliminate the conditions contributing to the insurgency?")

5. **Ask "why": Ask "why" of the initial problem statement. Then formulate a new problem statement based on the answer. Then ask "why" again, and again restate the problem based on the answer. Repeat this process a number of times until the essence of the "real" problem emerges.** Restating a problem several different ways is a divergent analytical technique that opens the mind to alternatives.

Source: Morgan D. Jones. The Thinker's Toolkit. New York: Three Rivers Press, 1995.

Step 3: Derive Elements of Own Mission

Any mission consists of two elements: the task(s) to be done by one's own forces and their purpose. There might be situations in which a commander has been given such broad guidance that all or part of the missions will need to be deduced. This is particularly true at a Strategic Command level. Deduction should be based on an appreciation of the general situation and an understanding of the superior's intent.

A task is the job or function assigned to a subordinate unit or command by higher authority. A mission can contain single or multiple tasks based on the complexity of the activity that is envisaged. There are two types of tasks:

1. Specified Task(s): Tasks listed in the mission received from higher headquarters are specified or stated (assigned) tasks. They are what the higher commander wants accomplished. The commander's specified tasks are normally found in the "Execution" section of the order but could also be contained elsewhere.

2. Implied Task(s): After identifying the specified tasks, the commander identifies additional major tasks necessary to accomplish the assigned mission. These additional major tasks are implied tasks that are sometimes deduced from detailed analysis of the order of the higher commander and an understanding of his intent, knowledge of the operating environment, or other factors that affect the mission. Implied tasks are subsequently included in the commander's restated mission and should be limited only to those considered essential to the accomplishment of the assigned mission.

Step 4: Identify Assumptions

An assumption is a supposition on the current situation (or a presupposition on the future course of events), either or both assumed to be true without positive proof, and necessary to enable the commander, during planning, to complete an estimate of the situation and decide the course of action. Assumptions can be made of friendly as well as hostile forces. Key characteristics of assumptions are that they are reasonable suppositions, both logical and realistic.

Assumptions are necessary in preparing a mission analysis. Within NATO, the political dimension of military operations is often a larger component of the planning process than in national capitals. This is a function of the decision-making structure within the Alliance. Assumptions concerning the degree of potential Alliance involvement or interest in an international event are crucial to effective intelligence preparation.

Step 5: Identify Objectives

Objectives are those elements that provide the link between the strategic through to the tactical levels of operations. A prerequisite for a good estimate of the situation is the identification of specific, realistic, and clearly defined objectives. The scope of NATO activities has changed considerably in the last decade. While NATO has been active in operations more during this time than ever before, considerable effort has been directed at non-traditional security activities to include the Partnership-for-Peace and Mediterranean Dialogue programmes. In many cases, NATO objectives will not be military in the traditional sense but rather political, particularly in a peace support operation. When assessing NATO objectives, it is important to understand the "soft security" concerns that affect the NATO Alliance. These include humanitarian, diplomatic, economic, and general stability concerns.

Section B: Primary Intelligence Requirement (PIR) Development

The mission analysis process produces a full appreciation of the likely extent of command interest in a particular intelligence problem. Mission analysis provides a list of likely tasks, both specified and implied, that must be completed. The provision of relevant intelligence products to support the completion of these tasks is the responsibility of the intelligence staffs. Intelligence planners must remain focused on the kinds of intelligence required to support the mission. Within a NATO context, OSINT is often the only source that can be tasked directly by the commander. The categories, types and level of detail required for intelligence analysis differ from echelon to echelon. Attempts to develop intelligence products beyond the scope necessary to support the mission will likely overburden the intelligence infrastructure with too much information, which could needlessly complicate the commander's decision-making process.

Mission analysis produces the Commander's Critical Information Requirements (CCIRs)[3]. These are those elements of information that are essential for the successful completion of his mission. A sub-set of CCIRs are his PIRs. PIRs are a focused list of command's critical intelligence needs. While this list should not be extensive, it should specifically identify the intelligence necessary to enable the commander to accomplish his mission. PIRs should be ranked in order of priority.

Using PIRs as the basis, the intelligence staff is able then to develop the command's information requirements – those items of information that must be collected and processed to develop the intelligence required by the commander. If the information does not already exist, then the intelligence staff must either issue a Request for Information (RFI) to a relevant intelligence provider or initiate the development of a collection plan.

[3] Commander's Critical Information Requirements (CCIRs) = Friendly Force + Enemy Force + Operating Environment. OSINT can support all three of these elements and the practical exploitation of open sources should not be limited solely to the Intelligence Staff.

Direction Development Worksheet[4]

1. **What is the Mission?**
 - Who
 - What
 - Where
 - When
 - Why

2. **What is the source of that Mission?**

3. **What is the commander's intent?**
 - Purposes of the force's activities
 - Desired results
 - How actions will progress toward that end

4. **What tasks must the command do for the mission to be accomplished?**
 - Specified tasks
 - Implied tasks

5. **What are the objectives?**
 - Political
 - Military
 - Economic
 - Social
 - Religious
 - Racial
 - Psychological
 - Environmental

6. **What are the Primary Intelligence Requirements (PIRs)?**

[4] This Direction Development Worksheet can be used to aid in the preparation of PIRs prior to the initiation of the collection planning process.

CHAPTER III: COLLECTION

Section A: Collection Planning

Collection Management

The Collection Management process consists of Information Requirements Management (IRM), Collection Planning, and Collection Coordination and Execution. The complexity of each is dependent on the capabilities and size of the organization. Collection Management usually begins with determining and sorting information requirements (discussed in the previous chapter). With a thorough knowledge of the capabilities of the available collection assets, the Collection Manager decides on the best means to satisfy the information requirements. He then constructs a Collection Plan and directs the execution of those collection activities. The Collection Manager will repeat the process if the requirement is still outstanding or if the collection was unsuccessful.

The Collection Manager in a multi-disciplined intelligence organization would determine what type of collection assets to place at what locations during what periods of time in order to have the greatest chance of acquiring the desired information (e.g., image, electromagnetic emission, acoustic event, verbal utterance, or text document).

Making a Collection Plan

Collection Planning lays out the most effective "what, where, and when" collection options in a way that matches each information requirement to a potential collection solution:

Information Requirement = What to Collect + What Collector + Where to Collect + When to Collect

Often, more than one collection solution is assigned to a single requirement in order to improve the odds of collecting quality data. Collection Plans are typically a matrix or spreadsheet with the three key pieces of information arranged in some graphic format. For example, different reconnaissance aircraft could be on the vertical axis, the time of flight on the horizontal axis, and the desired target of collection at the intersection.

An Internet Collection Plan

If the analyst's browser connected to the Internet is the only collection asset being considered, the collection planning process is still useful. The plan will save time and improve efficiency by keeping the collector focused on exactly what he is looking for.

- **Internet Location**
 A collection plan would match each Information Requirement with a location and time to collect from the Internet. In this case, the location is the server's URL or IP address and perhaps the details about how to access the site (i.e., password, drill downs, use site's search engine, etc.). To improve the chances of finding quality information or multiple pieces of supporting data, multiple sites may have to be collected against. There will be cases when a reliable site is already known and other times when the starting location will be a preferred search engine fine-tuned with key words and other specifications.

- **Time to Collect**
 The time dimension for collection may not be as obvious as location. Many news servers and indexing servers only keep information posted for a set amount of time before it is replaced by fresh information[5]. Some move the old information off to archives and others just delete it. For this reason, the Internet Collection Plan must include when and how often to look at the desired sites.

An Internet Collection Plan may look like this example:

Information Requirement	Site URL or IP	Access Details or Key Words	Search Time or Frequency
Blue Navy Exercise	http://www.janes.com/	Password & Naval Review	Archived by month
	https://portal.rccb.osis.gov/	Password & Exercise/Navy	Daily updates
Terrorist Bombing	http://www.msnbc.com/	Terror	Within 48 hrs
	www.alltheweb		
	http://www.ict.org.il	Background on terror organizations	Frequent updates

[5] For example, www.alltheweb.com indexes 3,000 news sources into a searchable database. Regrettably, it keeps this archive only for 48 hours.

The Internet Collection Planning Steps

The basic four steps to construct an Internet Collection Plan are as follows:

Step 1: Determine Searchable Information Requirements
Step 2: Determine Best Sites or Search Strategy
Step 3: Identify the Details to Access or Find Specific Information
Step 4: Determine Search Time Constraints

Step 1: Determine Searchable Information Requirements

Often, the Information Requirement as stated by the Commander (or other intelligence consumer) may not be in a form suitable for Internet searching. Sometimes the wording is too broad, too narrow, too vague, or consists of uncommon jargon. PIRs and other Information requirements are usually very broad and may need to be broken down into smaller, more specific information requirements for the Collection Plan. These are the Essential Elements of Information (EEIs) although there are many names and terms associated with this concept. A classic example is the Commander's PIR "indications of hostile intent." A search for hostile and/or intent will probably result in nothing found. That PIR may be turned into a series of possible component Information Requirements such as: Indications that Blueland is preparing for war, on heightened alert, or has improved their air defense readiness.

Step 2: Determine Best Site or Search

In many cases there will be one or more known reliable news or specialized web sites that you frequently refer to for information similar to what you are seeking. A good example is Janes International Defense Review for information about new military hardware and its use. You may decide to go directly to that site or use a service that searches a variety of journals and periodicals such as FACTIVA or LEXIS-NEXIS. For current events you probably have your favorite news sources such as BBC, CNN, or Mid East Newsline. Another option is to begin to search the web with a dependable search engine like AlltheWeb.com.

Step 3: Identify the Details to Access or Find Specific Information

As the step title states, the details needed to find the specific information may be of two different types: access and things that help you narrow down the location.

You may be going to a known site for which you are a registered user or subscriber and a login ID and password are required to gain access. Sometimes you can get away with using the same password and ID but often they are assigned randomly.

When you go to a known site or search engine, there are usually ways to get closer to the information you actually need. This could be by going to a sub-page, selecting a category, entering key words or search dates, etc. These will be covered in greater detail in the next section on search methods. To use an example of searchable keywords, let's go back to the hostile intent PIR from step 1. From such a vague PIR, a list of adversarial nations, their military leaders names, and words like heightened alert, improved readiness, forward deployed, and war preparations could be searched on to find resulting information that would reveal hostile intent.

Step 4: Determine Search Time Constraints

As mentioned above, current events information is perishable on web sites and many indexing servers. Some move the old information off to archives and others just delete it. It must be determined whether the sites need to be collected on several times each day, at least once per week, or whenever you get around to it depending on the priority of the requirement and refresh rate of the site. Newspapers and journals usually have archives but some require payment or a different means of access.

Using the Internet Collection Plan

Now that you have constructed a Collection Plan, it can be used by you or someone else to methodically locate and satisfy each of your Information Requirements or to identify those requirements that must be satisfied by another means.

Standing Requirements

Time spent in preparation will significantly increase the productivity of a research staff. Standing requirements such as INTSUM preparation or recurring reports can be templated so that the collection effort can be treated almost as a mechanical process. With an established collection plan supported by a report format, it is possible to quickly train staff to collect and prepare open source reporting in a standardized form.

Maintaining a dynamic collection of Internet links to support research, while time-consuming, is an efficient management tool. Link tables with supporting search terms and revisit advice can be built for all recurring tasks within an organization.

Internet Collection Plan

Priority Intelligence Requirement and Information Requirements	Key Terms	Sources to be Employed	Time to Collect	Remarks
1.				
2.				
3.				
4.				

Section B: Search Strategies

Search Methodology

Prepare Before You Search

The world of online resources to support your research is constantly expanding. Thus before delving into a search headfirst, it is best to consider your options. Online resources include:

- **Library catalogs**
 Most libraries have catalogs of their holdings. The majority of state and educational institutions' libraries are members of library consortiums, which allow you to search the member institutions' collections through their search engine. You can use this function to locate more difficult to find resources such as rare books, journals, magazines, etc.

- **Reference databases**
 These include encyclopaedias, periodical indexes, and full-text resources, which the library licenses from publishers for your use. Use these databases to identify (and read) articles on a variety of topics.

- **Internet resources**
 These are Internet search tools that are available to everyone. It is important to note, however, that a growing number of high-quality databases can be accessed via the Internet – but with a cost associated with their usage.

Because these resources are created by different organizations, they don't all look or function in the same way. The good news is that there are key searching skills that can be used in *all* of these online resources to help you connect quickly to the information you need. This section describes **six steps for successful searching.**

Step 1: Identify Key Concepts
Step 2: Identify Possible Search Terms
Step 3: Decide Which Method to Use To Search
Step 4: Construct Your Search
Step 5. Limit Your Search
Step 6. Refine Your Search

Step 1: Identify Key Concepts

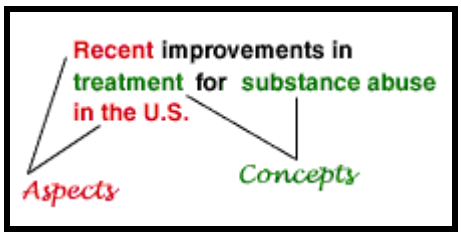
The key to successful searching is good preparation. There are two parts to this first step. First, before starting to search, take just a moment to analyse your search topic. Write a sentence describing what you are looking for. Then, second, identify:

1. The main concepts (Hint: these are usually nouns rather than verbs, adverbs or adjectives)

In the illustration below, the key concepts are "substance abuse" and "treatment."

2. Any aspects of the topic (such as time, place) that will be useful for focusing your research.

 In the illustration below some aspects are "recent" and "U.S."



Step 2: Identify Possible Search Terms

Next, make a list of words you can use to express each of your main concepts. As you do this, consider:

1. Are there narrower or broader terms you want to include in your search?

 For example, "substance abuse" is a broad concept. It can involve misuse of various kinds of substances, such as alcohol, drugs or tobacco. Each of these categories also has narrower aspects, as shown in the table below.

Broad term:	substance abuse		
Narrower:	alcohol	drugs	tobacco
Narrowest:	beer whiskey wine	cocaine heroin marijuana	cigarettes cigars snuff

2. What about **synonyms**? Are there different ways that your concept can be described? For example, some synonyms for "drug" are "dope, narcotic, opiate."

Often you may be able to think of synonyms, but you can also use a thesaurus to locate synonyms. There are even online sources like the *Wordsmyth Educational Dictionary - Thesaurus* (http://www.wordsmyth.net/), which can be of great assistance.

Topic Development Worksheet

The following worksheet acts as a useful tool to develop a specific topic from general concepts to specific search terms. Time spent thinking about a search before any keys are pushed can significantly increase search accuracy and completeness.

Topic Development Worksheet	
1. Name of topic, and what do you want to know about the topic:	
2. Spell out the topic: (Words, acronyms, abbreviations)	
Generic, simple terms	**Obscure, specific terms**
3. Make a list of "who" might publish such information (Industry associations, government agency, NGO's, user group etc)	

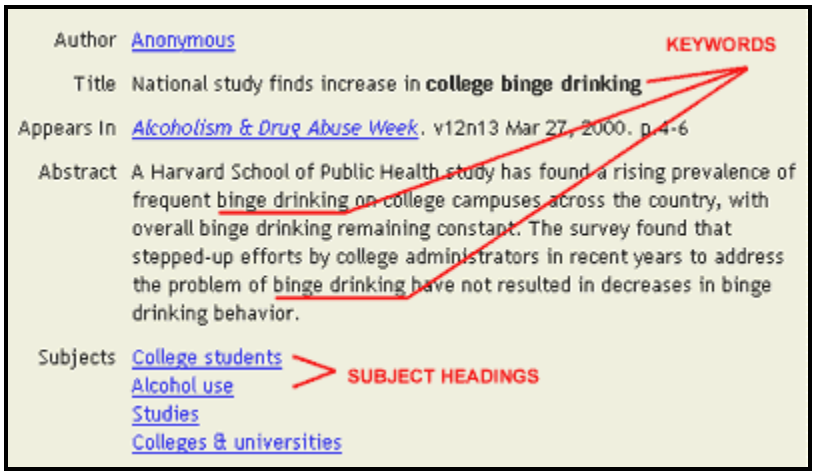
Step 3: Decide Which Method to Use To Search

The two most common methods of searching online sources are by subject and keyword. However there are also phrase, concept, and natural language searches.

1. **By SUBJECT**

 How: Using standard terms or "subject headings" that have been identified by an editor to represent the *main focus* of a document.

 Where: Library catalogs and most reference databases can be searched by subject. Indexes of web sites (like *Google* or *AltaVista*), however, do not have this feature.



 Efficiency: Subject searching is a precise (and thus efficient) method for finding information. It will help you find relevant information regardless of the varying terminology that different authors may use to describe a topic.

 Best Use: Because you can search with precision (and not retrieve unrelated information), use this method when your research topic is broad (such as "substance abuse") or ambiguous (such as "Columbus" -- do you need information about a city in Ohio or Christopher Columbus?)

Requirements: You must translate your search concepts into the subject vocabulary used by the database. Sometimes it is difficult to identify the correct subject terms. Also, the terms that work in one database may not be used by another (as shown below), so you should check the subject list ("thesaurus") for the database you are using.

Database:	**Thesaurus:**	**Subject Heading:**
OSCAR	Library of Congress Subject Headings	Substance abuse
Medline	Medical Subject Headings	Substance-related disorders
PsycINFO	Thesaurus of Psychological Index Terms	Drug abuse

2. **By KEYWORD**

How: Using words that may occur *somewhere* in a document, such as the title, description (abstract) or full-text of the resource itself.

Where: This method is used when searching web indexes. Library catalogs and reference databases also allow keyword searching.

Efficiency: Keyword searching is a less precise (and often less efficient) method for finding information. Because a keyword search looks at all of the words contained in a document (not just subject headings), it will find more results for you to sift through, and many may not be relevant.

Keyword searching also won't distinguish between different meanings. For example, if you want information about Turkey (the country), you will probably also find resources about turkey (the bird) mixed together in the results of a keyword search.

Best Use: Use keyword searching when your research topic is specific (such as "substance abuse during pregnancy") or not much has been written on it.

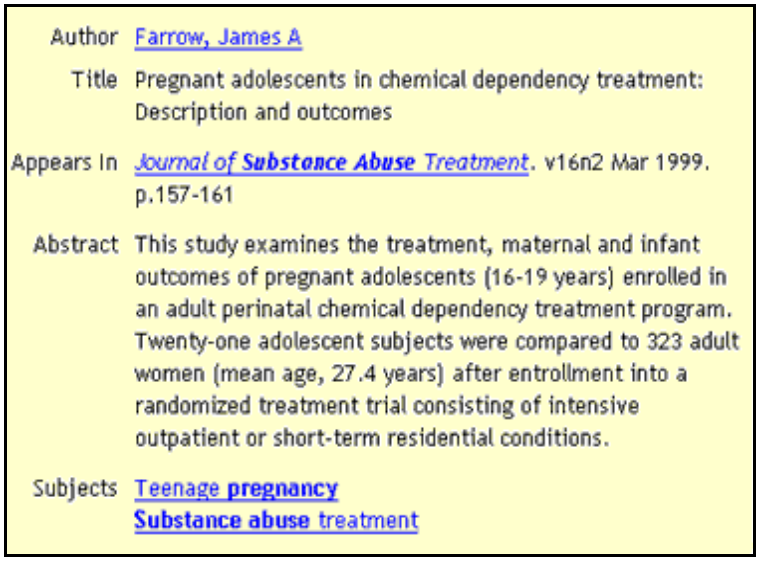
If a database allows both keyword and subject searching, you can also use keyword searching to identify subject headings when you are not sure which terms are used in that database to describe your topic. Skim results returned by a keyword search and find an item that looks useful. Then use a subject heading from that item in a new search by subject, in order to find more information on your research topic.

Requirements: You must construct a search statement if using more than one keyword. Your statement will use "operators" to connect search words. Various operators produce different effects.

EXAMPLE: Keyword Search in Library Database

The illustration shows a record found by a search in *Periodical Abstracts* for the keywords: substance abuse pregnancy

- "substance abuse" was found in both the journal title and the subject heading.
- "pregnancy" was found in another subject heading.



Author Farrow, James A

Title Pregnant adolescents in chemical dependency treatment: Description and outcomes

Appears In *Journal of* ***Substance Abuse*** *Treatment*. v16n2 Mar 1999. p.157-161

Abstract This study examines the treatment, maternal and infant outcomes of pregnant adolescents (16-19 years) enrolled in an adult perinatal chemical dependency treatment program. Twenty-one adolescent subjects were compared to 323 adult women (mean age, 27.4 years) after enrollment into a randomized treatment trial consisting of intensive outpatient or short-term residential conditions.

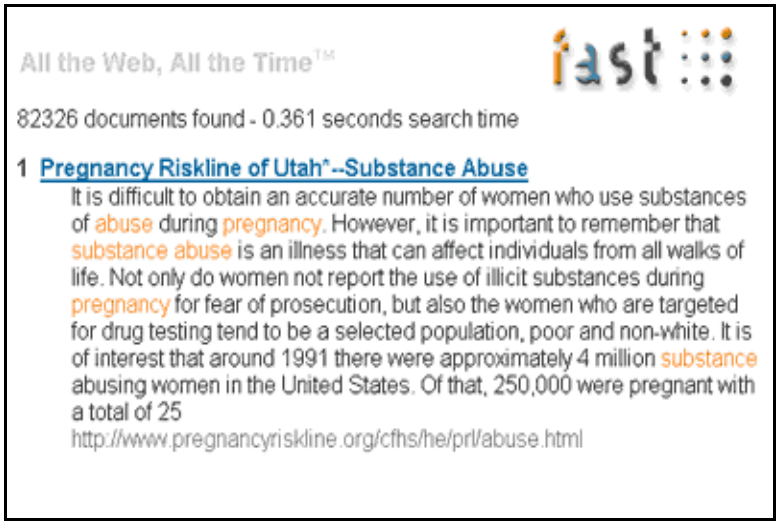
Subjects Teenage **pregnancy**
Substance abuse treatment

EXAMPLE: Keyword Search in Web Index

The illustration shows the first result found by a search in *FAST* for the keywords: substance abuse pregnancy

- "substance abuse" and "pregnancy" were both found in the web page title.
- these words were also found in the page text (they are highlighted in a lighter colour).

Since this is a web index, there are no subject headings that can be used to extend your search.



All the Web, All the Time™ fast

82326 documents found - 0.361 seconds search time

1 Pregnancy Riskline of Utah*--Substance Abuse
It is difficult to obtain an accurate number of women who use substances of abuse during pregnancy. However, it is important to remember that substance abuse is an illness that can affect individuals from all walks of life. Not only do women not report the use of illicit substances during pregnancy for fear of prosecution, but also the women who are targeted for drug testing tend to be a selected population, poor and non-white. It is of interest that around 1991 there were approximately 4 million substance abusing women in the United States. Of that, 250,000 were pregnant with a total of 25
http://www.pregnancyriskline.org/cfhs/he/prl/abuse.html

Step 4: Construct Your Search

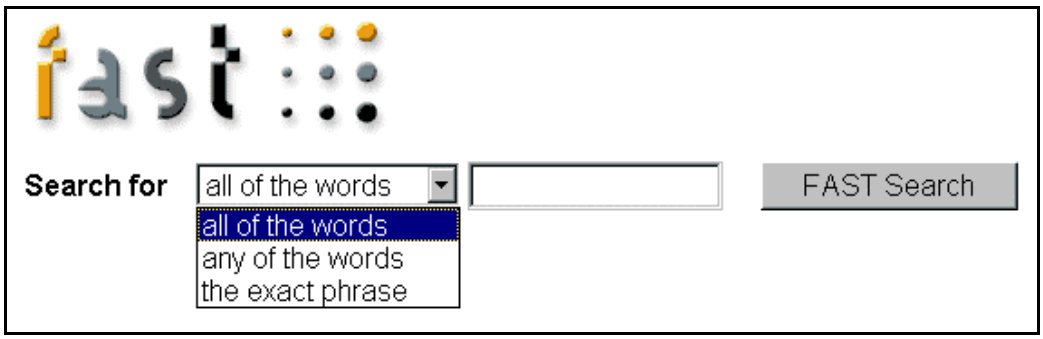
At this stage, you have identified main search concepts, developed a list of search words related to each concept, and chosen a method (subject or keyword).

With the keyword method, you can type a few search words and get results, but the outcome of this approach is unpredictable and often unsatisfactory. To perform an effective keyword search, you must formulate a search statement. This involves:

a. Selecting operators to connect your search terms
b. Identifying any search terms that are phrases
c. Deciding whether to include word variants
d. Organizing any complex search statements using parentheses.

a. Select Operators to Connect Search Words

There are several different types of "operators" that can be used to connect search words. Sometimes you will type these operators along with your search words into a search box. Sometimes you will select an option for connecting your search words from a pull-down list, like that shown in the illustration below.



Use Boolean Operators

Some databases use special connector words called Boolean operators to combine search terms. The most frequently used Boolean operators are: **AND, OR, NOT**.

Search for:	***What happens?***
addiction **AND** treatment	**requires** that **ALL** of these words be present in results; use AND to connect concepts
cocaine **OR** crack	**ANY** of these words can be present in results; use OR to connect synonyms
drugs **NOT** prescription	**excludes** words from results

Use Mathematical Operators

Some databases allow you to use either Boolean operators (words) or mathematical operators (symbols) to combine search terms. These mathematical operators are the **plus** symbol (+) and the **minus** symbol (-).

Search for:	***What happens?***
+addiction +treatment	**requires** that **ALL** of these words be present in results, like the Boolean operator AND.
+drugs -prescription	**excludes** words from results, like the Boolean operator NOT.

NOTE: Spacing counts. When constructing search statements using mathematical operators, be sure to format them correctly, so that the search works as intended:

- DON'T leave a space between the math symbol and your search word.
- DO leave a space between each element (symbol plus search term).

Be Consistent

Use either words or symbols as operators in your search statement. Don't mix them together.

Correct usage: +addiction +treatment
Incorrect usage: +addiction AND treatment

Implied Operators

What happens if you don't use any operators? In many databases, one of the Boolean operators (AND or OR) is implied and thus is supplied automatically by the system. ***There is no standard for this, so you must check the database HELP pages to find out which operator is implied.***

b. Identify Search Terms that are Phrases

When constructing a search statement, it is important to identify any words that should be considered a phrase. Online sources use various methods for phrase searching. Depending on the database, you may be required to:

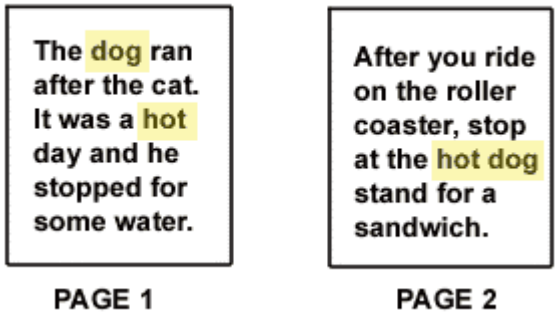
1. Use **quotation marks** to enclose an **exact phrase**
2. Choose the phrase search option from a **drop down menu**
3. Use a **Boolean operator** such as **NEAR** or **ADJ** to indicate **proximity** of terms

Search for:	***What happens?***
substance **NEAR** abuse	finds both words near each other (often in the same sentence), in **any order**. This search will find the exact phrase "substance abuse" as well as the phrase "abuse of a controlled substance."
substance **ADJ** abuse	finds both words next to (adjacent to) each other, in **any order**.
"substance abuse**"**	both words together in this **exact order**.

NEAR and ADJ are useful Boolean operators, but they are not universally supported by all databases. If they are available in the database you are using (check HELP to find out), use NEAR or ADJ instead of quotation marks when you are not sure of the order of the words in a phrase.

Note that phrase or proximity searching is more restrictive than using the AND operator. Using quotation marks around an exact phrase or the ADJ operator between

words that form a phrase will produce smaller, more precise results, but not always more accurate. Without care, use of these search techniques may narrow your search excessively.



Example:

- Search for: **hot AND dog** will find both pages 1 and 2 in the illustration above.
- Search for: **"hot dog"** or **hot ADJ dog** will find only page 2.

Summary

The table below summarizes the effect that various operators will have on your search results, from least restrictive (producing the biggest set of results) to most restrictive (producing the smallest set of results).

Operator:	***Example:***	***Web Search Results***
OR	peanut OR butter OR cookies	1,499,578 pages
AND (or plus sign)	peanut AND butter AND cookies	33,534 pages
NEAR	peanut NEAR butter NEAR cookies	10,591 pages
ADJ	peanut ADJ butter ADJ cookies	5,291 pages
phrase indicator	"peanut butter cookies"	3,838 pages

To find recipes for peanut butter cookies, for example, the most efficient search statement is:

Using Boolean operators: "peanut butter cookies" AND recipes
Using mathematical operators: +"peanut butter cookies" +recipes

c. Include Variant Forms of Search Words

Many databases execute searches quite literally. If you search for the singular form of a word (such as cat), the plural form (cats) will not be found. But often databases have a **wildcard** feature that you can use to find variant forms of your search words.

Generally, you must include some symbol, such as the question mark (**?**) or the asterisk (*****) at the end of word roots to find plural and related forms. Check database HELP pages to find out which symbol is used.

Example:

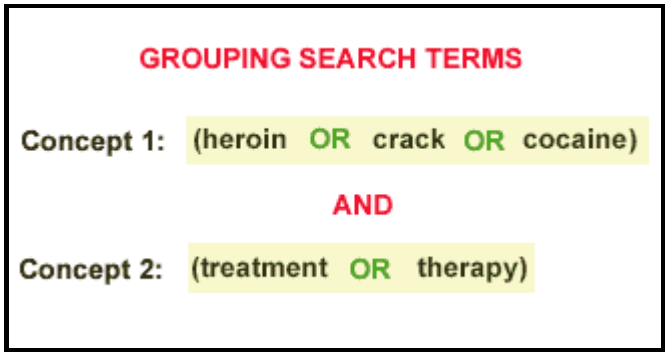
- Search for: substance**?** NEAR abuse**?**
- Will find: substance abuse, substance abuser, abuse of controlled substances

Some databases have a **stemming** feature that solves the problem of variant word forms. They will automatically search for "cat" if you enter the keyword "cats" and vice versa.

d. Use Parentheses to Group Search Words

It is also possible to create more complex search statements by using parentheses to group search words that should be treated in the same way. This is sometimes called "nesting" and is a handy way to incorporate **synonyms or related terms** into your search.

As the illustration below shows, you may link synonyms or related terms for each of your search concepts into a "cluster" using the OR operator. Enclose a cluster within parentheses. You can then combine clusters using the Boolean operator AND.



At least some of the words from *each* of the concept clusters should be represented in the results for this search.

e. Recommended Strategies for Keyword Searching

- **Perform your search in stages**. First, search for the most important concepts or the most unique words (those least likely to occur in search results). Then look over your results and decide whether you need to change anything. Don't begin with search statements that are complex and elaborate. Rather, build from a simple beginning.

- **Keep phrases short**. Longer phrases are less likely to be found. For example, search for "substance abuse" AND treatment, not "substance abuse treatment programs."

- **As you review results, watch for new or alternate terms**. Incorporate them into your next search. For example, use "chemical dependency" as well as "substance abuse." Connect these search terms with the OR operator to expand your results.

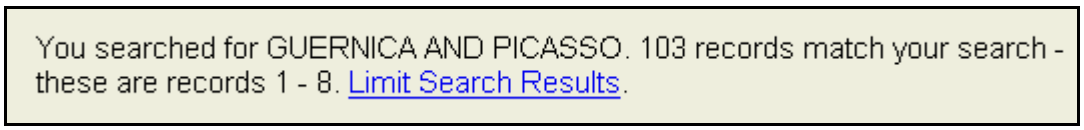
Step 5. Limit Your Search

A search often returns much more information than you can possibly use. Previously, we saw that by choosing the most appropriate operator, you can produce better results. Most online databases also allow you to limit (screen) your search results to improve them. But the specific criteria that you may use to limit your search will vary.

Library catalogs and many reference databases offer different criteria or variables that can be used to limit your search results. Typically, you can limit by:

- Language
- Media or material type
- Time frame or publication date

Pre-Limit or Post-Limit? Some library catalogs and databases allow you to set up limits on the original search form (pre-limit) as well as after the initial search has returned results (post-limit). To post-limit, look for a "Limit" link or button on the search results page, like the one in the illustration below.



Usually, **post-limiting works best**. First, try your search without any limits to see what results are produced. Then, if there are too many to review quickly (more than 2 pages), post-limit the search results by some variable that seems most relevant.

Examples:

- If your results are in many different languages, try limiting to English language only.
- If your results should be recent, try limiting by publication date.

Limiting in a Web Index

When searching a web index, some of the same limiting criteria (such as language) may be available. However, in a web Index you may also limit your search to various elements present in web pages, such as:

- **Page titles**
- **Headers**
- **URLs**

If your search terms are found in these key parts of a web page, it is more likely to be relevant to your needs.



Example: Web Index

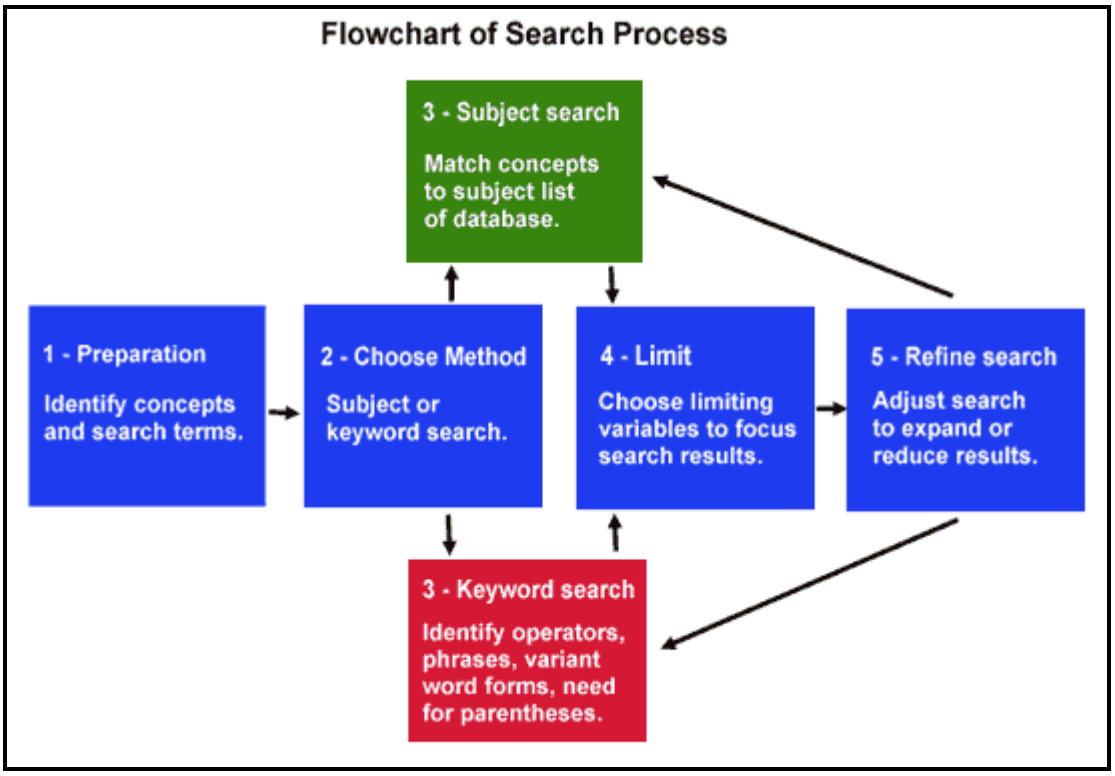
The example on the right shows a search in Google, a web index, for the phrase "Ohio State Buckeyes." By limiting this search to page titles, we will find sites that have this topic as their main focus.

The net.TUTOR tutorial on "Using Web Search Tools" provides more information on how to use the limiting feature in web indexes.



Step 6. Refine Your Search

Searching can be unpredictable. Some searches return too much information. Sometimes a well thought out search just doesn't find enough information. In any event, most online searching is "iterative," requiring that you continually refine or tune your search, as shown in the illustration below.



Here are some proven strategies for adjusting keyword searches that find too much or too little.

Adjust:	**To Narrow Results:**	**To Expand Results:**
SEARCH CONCEPTS	**Add** search concepts, using the AND operator.	**Remove** some search concepts. Find information on the most important concept first.
SEARCH WORDS	**Remove** some search words, especially vague, ambiguous or abstract words.	**Add** more search words, using the OR operator.
SEARCH FOCUS	**Limit** search focus to a specific field or aspect (date, language, media, etc.)	**Broaden** the search focus from subject to keyword, or from one field to all fields of database.

Example:

- **Initial search:**
 "substance abuse" AND treatment
- **Too many results? Narrow by adding new concept:**
 "substance abuse" AND treatment AND Ohio
- **Too few results? Expand by adding more search words:**
 ("drug abuse" OR alcohol OR alcoholism OR "substance abuse") AND (treatment OR therapy)

Section C: Search Worksheet

1. Spell it Out

Spell-out the subject you are searching for. Write down any buzzwords, acronyms and abbreviations. Be sure the think about the "who" associated with your subject. Who would be likely to produce or publish the information you are seeking? Is there a well-known expert, university or association that specializes in your subject? The words you write down become the basis for keyword searches later on. For example; a search for anti-ship missile information might involve the following terms; missile, cruise-missile, sea-based weapons, Harpoon, Silkworm, USNI ("United States Naval Institute"), etc.

2. Strategize - Choose your approach, which online resources, tools

Consciously decide what are the best online tools to use for each of your specific search terms. This requires that you understand that there are different strengths and weaknesses of the various online tools.

- Subject Tree (Yahoo) - Use for general terms and subject keywords only (i.e. cancer).
- Search Engines: (Alta Vista) - Use for detailed, obscure keywords. (i.e. Coetaneous T-Cell Lymphoma/Mycosis Fungicides)
- Virtual Libraries (Joe's Ultimate guide to XYZ,) - Seek out virtual libraries, if you need an in-depth guide for your subject. (i.e. OncoLink)
- Online Communities (Dejanews) - Use when you are looking for other people's opinions (i.e. alt.support.cancer, sci.med.diseases.cancer)
- Specialized Tools - There are many specialized tools, which can take you to another level of detail. These tools can quickly answer searches within their area of expertise. For example:
 - "What is John Doe's Phone number, address, directions to his house, and a listing of all his neighbour's names, phone numbers and addresses?" (See Anywho)
 - "Show me a list of the antique dealers nearest Anytown, US. (see Switchboard)
 - Who are the biggest polluters in my county? (See Scorecard)

3. Search - Get online, execute, stay focused, use advanced search features

Your search results depend greatly on how you phrase your keywords. First, be sure you are asking the appropriate level of detail for the specific tool you are using (general words at Yahoo, obscure words and specific phrases at Alta-Vista). You can focus your results when you take the time to read the help file and construct a more specific query.

4. Sift - Filter the results, Follow the leads

You may be presented with many search results and potential leads. Stop and read, before you click and waste time. Scroll up and down the entire page, and determine which are the most promising links based on the descriptions. Before you click on a link, hover over the link, and read the link's URL in the browser's feedback area (at the bottom of the screen). You will be surprised how many dead-end links you will avoid just by reading their URLs first. Finally, whenever you see 2 or more interesting links to pursue, go ahead and explore all of them simultaneously by opening multiple web browsers.
As you look through the search results, you should also be taking notes of new information that you will use in future iterations of your search.

5. Save

When you discover a great site, be sure to save this discovery, or you are doomed to repeat the search all over again. Methods of saving include:

- Add a bookmark, and organize your bookmarks into folders/submenus.
- Save a copy of the page to disk using "file" --> "save as".
- Copy and paste selected text directly from the web page into a word processing program. You may also want to copy and paste the URL into the word processor, so later on you will know where the page came from.

Summary - Take the time to think about your searches, otherwise you can waste a lot of time.

Section D: Search Tools

Search Engines

What are search engines?

Search engines are huge databases of web page files that have been assembled automatically by machine.

There are two types of search engines:

- *Individual*. Individual search engines compile their own searchable databases on the web.
- *Meta*. Metasearch engines do not compile databases. Instead, they search the databases of multiple sets of individual engines simultaneously.

How do search engines work?

Search engines compile their databases by employing "spiders" or "robots" ("bots") to crawl through web space from link to link, identifying and perusing pages. Sites with no links to other pages may be missed by spiders altogether. Once the spiders get to a web site, they typically index most of the words on the publicly available pages at the site. Web page owners may submit their URLs to search engines for "crawling" and eventual inclusion in their databases.

Whenever you search the web using a search engine, you're asking the engine to scan its index of sites and match your keywords and phrases with those in the texts of documents within the engine's database.

It is important to remember that when you are using a search engine, you are NOT searching the entire web, as it exists at this moment. You are actually searching a portion of the web, captured in a fixed index created at an earlier date.

Thus, how much earlier is an important aspect to consider when using a search engine. Spiders regularly return to the web pages they index to look for changes. When changes occur, the index is updated to reflect the new information. However, the process of updating can take a while, depending upon how often the spiders make their rounds and then, how promptly the information they gather is added to the index. Until a page has been both "spidered" AND "indexed," you won't be able to access the new information. Thus, the more often a spider checks for changes, the more accurate the search returns for that page will be.

The accuracy of your search is directly proportional to how many web pages the search engine indexes. The more web pages the engine indexes, the more accurate your search. Also, the accuracy of your search also depends on how often the search engine indexes web pages. The more often a search engine indexes web pages, the more accurate your search will be.

What are the pros and cons of search engines?

On the pro side, search engines are the best means devised yet for searching the web. Stranded in the middle of this global electronic library of information without either a card catalogue or any recognizable structures, how else are you going to find what you're looking for?

On the down side, the sheer number of words indexed by search engines increases the likelihood that they will return hundreds of thousands of irrelevant responses to simple search requests. Remember, they will return lengthy documents in which your keyword appears only once. Secondly, the vastness of the Internet means that no search engine can possibly actually search all of it. Technology may change this in the future, but as of now, even the most comprehensive search engine (Google) only covers a fraction of the entire web. Another problem with search engines is what is called the "invisible" or "deep" web. For details on the "invisible" web see the section "Searching the Invisible Web."

Are search engines all the same?

NO. Search engines use proprietary software programs to search their indexes for matching keywords and phrases, presenting their findings to you in some kind of relevance ranking. Although software programs may be similar, no two search engines are exactly the same in terms of size, speed and content; no two search engines use exactly the same ranking schemes, and not every search engine offers you exactly the same search options. Therefore, your search is going to be different on every engine you use. The difference may not be a lot, but it could be significant. Recent estimates put search engine overlap at approximately 60 percent and unique content at around 40 percent. Thus, it is VERY important to carefully consider how a particular search engine compiles its results when conducting Internet searches.

How do search engines rank web pages?

In ranking web pages, search engines follow a certain set of rules. These vary from one engine to another. Of course, the goal of all of them is to return the most relevant pages at the top of their lists. To do this, they look for the location and frequency of keywords and phrases in the web page document and, sometimes, in the HTML metatags. They check out the title field and scan the headers and text near the top of the document. Some of them assess popularity by the number of links that are pointing to sites; the more links, the greater the popularity, i.e., value of the page. Because they vary greatly, it is crucial to understand how a particular search engine ranks results. For example, if you were searching on a current events related topic, a search engine that ranks results by date would be extremely useful.

When do you use search engines?

Search engines are best at finding unique keywords, phrases, quotes, and information buried in the full-text of web pages. Because they index word by word, search engines are also useful in retrieving tons of documents. If you want a wide range of responses to specific queries, use a search engine.

Note: Today, the line between search engines and category search engines is blurring. Search engines no longer limit themselves to a search mechanism alone. Across the web, they are partnering with subject directories, or creating their own directories, and returning results gathered from a variety of other guides and services as well. One example is Google's (a search engine) teaming with Open Directory (http://www.dmoz.org/) to categorize search results.

A note on metasearch engines.

Use metasearch engines at your own risk for while they do have certain advantages (i.e. they can cover a large number of search engines in a single search), they have many weaknesses. These weaknesses include: most don't search all of the largest engines, most don't give you more than 10 records from each search engine, and most list paid listings first. The best way to demonstrate the weakness of metasearch engines is through the following example.

Caption 1. Search for: *"geologic resources" worcester* via search engines directly versus metasearch engines

	Done Directly	via *DogPile* (Results per site)	via *metacrawler.com* (Results per site)	via *search.com* (Results per site)
Google	39	0	0	0
AllTheWeb	40	0	0	0
HotBot	15	0	0	0
Alta Vista	9	0	0	2

Search Options Offered by Selected Search Engines

Feature	Search Engine
Boolean operators	AltaVista Advanced Search (http://www.altavista.com/) C4 (http://www.c4.com/) Dogpile (http://www.dogpile.com/) HotBot (http://www.hotbot.com/) Ixquick Metasearch (http://www.ixquick.com/) ProFusion (http://www.profusion.com/) WebCrawler (http://www.webcrawler.com/)
Full Boolean logic with parentheses, e.g., *behaviour and (cats or felines)*	AltaVista Advanced Search (http://www.altavista.com/) C4 (http://www.c4.com/) HotBot (http://www.hotbot.com/) Ixquick Metasearch (http://www.ixquick.com/) MSN Search Advanced Search (http://search.msn.com/advanced.asp)
Implied Boolean +/-	Most search engines offer this option
Boolean logic by template terminology	AllTheWeb Advanced Search (http://www.alltheweb.com/advanced) AOL.COM Search Options (http://search.aol.com/refine.adp) HotBot (http://www.hotbot.com/) Lycos Pro (http://lycospro.lycos.com/) MSN Search Advanced Search (http://search.msn.com/advanced.asp) ProFusion Advanced (http://www.profusion.com/) Snoopa (http://www.snoopa.com/)
Proximity operators	AltaVista Advanced Search (http://www.altavista.com/) Google (http://www.google.com/) Ixquick Metasearch (http://www.ixquick.com/)

Search Engine Guide: The following charts provide a snapshot of the features provided by various search engines as of May 2002. Familiarity with the features and strengths/weaknesses of each can radically improve the accuracy of the search results returned.

Major Search Engine – Features Guide - 2002

	All The Web	All the Web Advanced	Alta Vista Advanced	Alta vista Advanced
URL	http://www.alltheweb.com/	http://www.alltheweb.com/advanced	http://www.altavista.com/	http://www.altavista.com/sites/search/webadv
SIZE (pages)	600 million	600 million	500 million	600 million
SIMPLE BOOLEAN	*term* *-term* *defaults to an AND*	*(menu)* *+ term* *-term*	*Term* *-term* *Defaults to an OR*	Defaults to phrase
FULL BOOLEAN_	(term] term2) equals an OR			OR AND AND NOT ()
PHRASE	(menu) " "	(menu) " "	" " some automatic	" " automatic
PROXIMITY				NEAR (= within 10 Words)
TRUNCATION			*term* (asterisk - internal or at the end of term)*	*term* (asterisk - internal or at the end of term)*
TITLE FIELD		(menu)	title: term	title: term
DATE FIELD		menu		(date range boxes)
URL FIELD		(menu)	url: term domain: term host:term	url: term domain: term host:term
"LINKS TO" A URL		(menu)	link:term	link:term
LANGUAGE		(menu)	(menu)	(menu)
MEDIA SEARCHING	Links to News, Pictures, Videos, MP3, FTP Searches	News, Pictures, Videos, MP3, FTP all have their own advanced mode	Links to Media searches image : term	image : term
CASE SENSITIVE			yes	yes
SEARCH ALL COMMON WORDS	yes	yes	yes	yes
WEB DIRECTORY ATTACHED			yes LookSmart	
CLUSTERED RESULTS	no	no	yes	yes
OUTPUT OPTIONS	standard	standard 10, 25, 50, 75, 100	Standard Customizable	standard one result per website 10, 20, 30, 40, 50 results customizable
PAID SITES FIRST	no	no	yes	yes
SIMILAR PAGES			yes	yes
ALSO SHOWN ON RESULT PAGES			"Others searched for Headlines"	"Others searched for Headlines"
OUTSTANDING SPECIAL FEATURES	Largest multimedia search Adult content filter Fast, extensive news search FTP search	Adult content filter	Images/ audio/ video search Translations Adult content filter Hit terms Highlighted	Images/ audio/ video search Translations Adult content filter

	Excite Home	Google	Google Advanced
URL	http://www.excite.com/	http://www.google.com/	http://www.google.com/advanced_search?hl=en
SIZE (pages)	330 million	3 billion, not all fully-indexed	3 billion, not all fully-indexed
SIMPLE BOOLEAN	*Term* *-term* *defaults to an OR*	*-term* *defaults to an OR*	*(text boxes)* *defaults to an AND*
FULL BOOLEAN	AND OR NOT [?] ()	OR	
PHRASE	" "	" "	" " (text boxes)
PROXIMITY			
TRUNCATION	automatic		
TITLE FIELD			
DATE FIELD			
URL FIELD			
"LINKS TO" A URL		link:term	link:term
LANGUAGE			(menu)
MEDIA SEARCHING	"Photos" radio button		Image Search Box
CASE SENSITIVE			
SEARCH ALL COMMON WORDS		No, but can force it with a+	No, but can force it with a+
WEB DIRECTORY ATTACHED	yes Look Smart	yes link to open directory	
CLUSTERED RESULTS	no	yes	yes
OUTPUT OPTIONS	Titles Titles & Summaries Grouped by URL	10, 20, 30, 50, 100 Results	10, 20, 30, 50, 100 Results
PAID SITES FIRST	no	no	No, but can force it with a+
SIMILAR PAGES		yes	yes
ALSO SHOWN ON RESULT PAGES	Directory hits Related searches ("Zoom in") stock and company information links Travel links etc.	Open Directory categories and sites Link to cached page Translation option Stock Quote option Link to definitions, Maps Headlines Address & phone #s	Open Directory categories and sites Link to cached page Translation option Stock Quote option Link to definitions, Maps Headlines Address & phone #s
OUTSTANDING SPECIAL FEATURES	Concept Searching News search Hit terms highlighted	Ranking based on "link" popularity Newsgroups & images Cached pages Adult content filter Covers PDF & other formats	Ranking based on "link" popularity Newsgroups &images Cached pages Adult content filter Covers PDF & other formats

	Hot Bot	Hot Bot Advanced	Lycos	Lycos Advanced
URL	http://www.hotbot.com/		http://www.lycos.com	http://search.lycos.com/adv.asp
SIZE (pages)	230 million	230 million	Uses the Fast Search database - 600 million	Uses the Fast Search database - 600 million
SIMPLE BOOLEAN	*(menu) term -term defaults to an AND*	*(menu) term -term defaults to an AND*	*Term -term defaults to an AND*	*(menu) term -term defaults to an AND*
FULL BOOLEAN_	OR AND NOT () (Must also use menu)	OR AND NOT () (Must also use menu)	(term 1 term 2) equals an OR	(term 1 term 2) equals an OR
PHRASE	(menu) " "	(menu) " "	" "	(menu) " "
PROXIMITY				
TRUNCATION		"Stemming" option		
TITLE FIELD	(menu) title: term	(menu) title: term		(box under "Link Referrals"tab)
DATE FIELD	(menu)	(menus)		
URL FIELD	(menu) domain: term	(menu) domain: term (Region menu)		(boxes, under "Page Field" tab)
"LINKS TO" A URL	(menu)	(menu)		(boxes, under "Link Referrals" tab)
LANGUAGE	(menu)	(menu)		(radio buttons under "Language" tab)
MEDIA SEARCHING	(checkboxes)	(checkboxes)	Links to "Multimedia" search	(radio button)
CASE SENSITIVE				
SEARCH ALL COMMON WORDS			yes	yes
WEB DIRECTORY ATTACHED	yes Open Directory		yes Open Directory	(link to Open Directory)
CLUSTERED RESULTS	yes	yes	no	no
OUTPUT OPTIONS	Full, brief, URL's only 10, 25, 50, 100, results from this site only	Full, brief, URL's only 10, 25, 50, 100, results from this site only	standard	standard
PAID SITES FIRST	yes	yes	yes	no
SIMILAR PAGES				
ALSO SHOWN ON RESULT PAGES	Related searches Direct Hit popularity results (top 10) Directory categories Travel links Stock links	Related searches Direct Hit popularity results Directory categories Travel links, Stock links	Reviewed sites Directory hits Links to quotes, news, travel links, etc. Matching news and shopping items Related searches	
OUTSTANDING SPECIAL FEATURES	Direct Hit popularity results	Direct Hit popularity results Search by region	Hit terms Highlighted Adult content filter	Adult content filter Downloads,MP3, news, newsgroups, etc. Hit terms Highlighted

	Teoma	WiseNut	Yahoo!
	http://www.teoma.com/	http://www.wisenut.com/	http://www.yahoo.com/
SIZE (pages)	200 million?	1.5 billion	1-2 million in directory (est.), 6m from Google
SIMPLE BOOLEAN	*term -term defaults to AND*	*term -term defaults to AND*	*+term -term defaults to AND*
FULL BOOLEAN_			
PHRASE	" "	" "	" "
PROXIMITY			
TRUNCATION			Automatic term* (asterisk)
TITLE FIELD			term
DATE FIELD			(menus under "Advanced Search"))
URL FIELD			u:term
"LINKS TO" A URL			
LANGUAGE		(menu on Set Preferences page)	
MEDIA SEARCHING			
CASE SENSITIVE			
SEARCH ALL COMMON WORDS	yes		
WEB DIRECTORY ATTACHED			Primarily is a directory
CLUSTERED RESULTS		yes	no
OUTPUT OPTIONS		standard	standard (Advanced search allows choose of 10, 20, 50, 100)
PAID SITES FIRST			no
SIMILAR PAGES			
ALSO SHOWN ON RESULT PAGES	Categories Expert's Links		Categories Directory hits Google hits, news, web events Links to stock quotes, news, etc. Related searches
OUTSTANDING SPECIAL FEATURES	Expert's Links	Automatic categorization of results	Hit terms Highlighted Automatic transfer of "no hits" search to partial Google

Source: Ran Hock, Online Strategies, www.onstrat.com

Search Tools

Copernic

Rather than laboriously employing a number of search engines individually in order to cast a wider net, there are a number of meta-search engines that will simultaneously search a number of sources and return a consolidated response. One of the best known of these is Copernic 2001. It is available from www.copernic.com.

The free version of Copernic searches most of the major search engines. The full version adds a number of categories including *newsgroups* to the customized list of search engines that it employs. In addition it also allows the user to search in different languages and in specific countries. Copernic can also be used to automatically update searches and provide results ready for analysis upon arrival in the office.

Deep-Web/Invisible Web

Searching the Invisible Web

The *invisible web* is composed of web pages that can be accessed via the Internet, but are not found by search engines. These are pages that are either located too "deep" in a web site for a search engine's spider to locate, are pages that a search engine cannot index because it technically can't do so, or are pages which the search engine cannot access because they lack the proper password.

In 1994, Dr. Jill Ellsworth first coined the phrase "invisible Web" to refer to information content that was "invisible" to conventional search engines. Perhaps a more appropriate term is "The Deep-Web" as most of this content resides in searchable databases, the results from which can only be discovered by a direct query. Without the directed query, the database does not publish the result. When queried, deep Web sites post their results as dynamic Web pages in real-time. Though these dynamic pages have a unique URL address that allows them to be retrieved again later, they are not persistent.

Search engines — the primary means for finding information on the "surface" Web — obtain their listings in two ways. Authors may submit their own Web pages for listing, generally a minor contributor to total listings. Or, search engines "crawl" or "spider" documents by following one hypertext link to another. Simply stated, when indexing a given document or page, if the crawler encounters a hypertext link on that page to another document, it records that incidence and schedules that new page for later crawling. Like ripples propagating across a pond, in this manner search engine crawlers are able to extend their indexes further and further from their starting points.

Thus, to be discovered, "surface" Web pages must be static and linked to other pages. Traditional search engines cannot "see" or retrieve content in the deep Web, which by definition is dynamic content served up in real time from a database in response to a direct query. Public information on the deep Web is currently 400 to 550 times larger

than the commonly defined World Wide Web. The deep Web contains 7,500 terabytes of information, compared to 19 terabytes of information in the surface Web.

The deep Web contains nearly 550 billion individual documents compared to the 1 billion of the surface Web. More than an estimated 100,000 deep Web sites presently exist. Sixty of the largest deep Web sites collectively contain about 750 terabytes of information – sufficient by themselves to exceed the size of the surface Web by 40 times.

There are several web sites dedicated to searching the invisible web. The most comprehensive of these is Direct Search, maintained by Gary Price, a reference librarian at the George Washington University, in Washington, DC and the author of "The Invisible Web." These sites also contain more information on the invisible web itself. Note that these sites are mostly directories of sites and not individual sites. Therefore, one should be prepared to cast their search net very broadly by topic area.

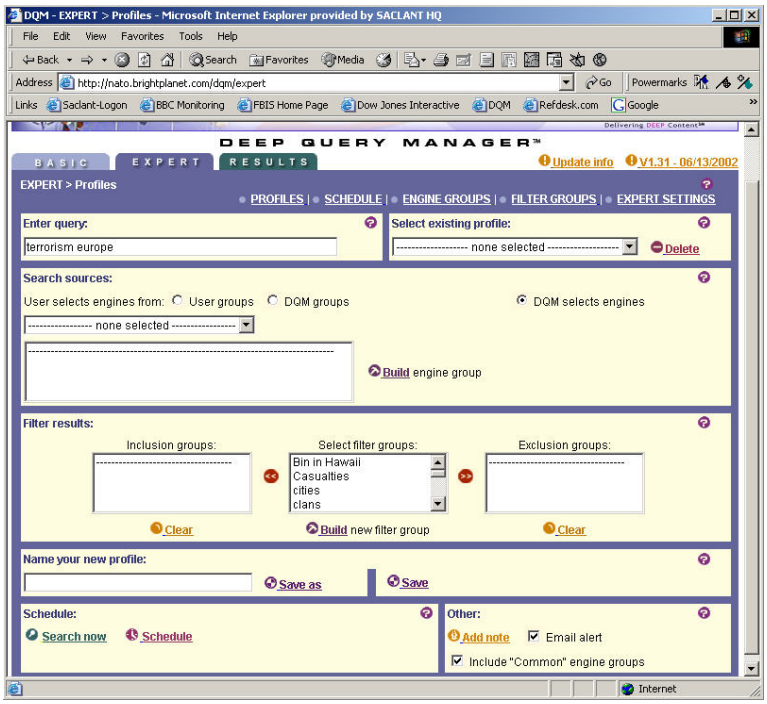
- Direct Search - http://www.freepint.com/gary/direct.htm
- Invisible Web (based on the book) – http://www.invisible-web.net/
- Invisible Web.com – http://www.invisibleweb.com/
- Complete Planet – http://www.completeplanet.com/

Deep Query Manager

In order to reach these sites in an efficient manner a specialized tool is required. Deep Query Manager is a web-based search service that enables effective access to the Deep Web. It was produced and maintained by Bright Planet of Sioux Falls, SD.

Deep Query Manager provides the means with which to search literally thousands of Deep Web sites simultaneously with the same query, providing a consolidated return of results based on document relevance. The service provides a number of other useful features including:

- The conduct of searches with a degree of anonymity through the use of Bright Planet's third-party server.
- The customizing of specific search sources based on topic parameters.
- The ability to compare results of consecutive searches on the same sources to return only the new documents.
- The capability to share search results with other analysts within your organization through the share results feature.



Deep Query Manager can run a variety of searches simultaneously. Search completion is notified via an email alert. While even a service like Deep Query Manager can take some time to search thousands of web sites, it is able to conduct many searches simultaneously thus increasing overall efficiency.

Deep Query Manager also has a scheduling function. This is useful for repetitive searches. Searches can be scheduled for completion prior to the start of the workday so that there is no waiting time prior to the commencement of analysis.



The capabilities provided in a product like *Deep Query Manager* provide two key benefits: a higher degree of confidence that a greater number of available information sources have been tapped, and; efficient use of technology to reduce repetitive tasks thus increasing the time available for analysis of the collected information.

Section E: Searching Anonymously On The Web

General

Why would anyone want to search anonymously on the Web? All the information on the Web is freely available to anyone with a PC and a connection. The answer lays not so much in people identifying who we are but, without a few precautions, we might give away our intentions and shut down what may become valuable sources of information.

There are strong arguments in favour of not hiding our presence on the Web. Some would argue that to enhance security and co-operation we should be as open as possible. This is a very strong argument but ignores the fact that some security will always be necessary. An obvious presence on the Web actually helps our own security because it means we can only apply specialised and anonymous search techniques only when and where they are really needed.

Being anonymous on the Web may not necessarily involve deception. It is quite possible to surf the Web without openly identifying your identity, purpose or intentions. This is simply a case of 'I won't tell you unless you ask'. There may be occasions when you will want to communicate with someone without using your real name. These occasions should be rare and should be assessed individually.

Don't leave yourself open to attack

Before you even start surfing anonymously make sure you don't leave your Internet connection open to attack. You may take all the precaution necessary to hide your intentions and identity whilst surfing, but if all the sites that you have visited and all the information you have downloaded is stored on your PC and available via your open connection, then you are vulnerable.

There is an argument for the use of a firewall to stop hackers at the front door, but remember that there hasn't been a firewall yet that wasn't eventually cracked. The very expensive firewalls do a good job but it is unlikely that you would want to spend so much money for a simple Internet connection. Besides if you wanted to remain anonymous on the Internet an expensive firewall is not the way to do it. It would highlight the fact that you had something to hide. The same argument applies to the cheaper firewalls. Because they are cheap they are also vulnerable. Hackers know how to get in and often see areas with firewalls as a challenge.

Possibly the best security is to remain anonymous and look just like everyone else. By doing this, if a hacker chooses to attack your Internet connection whilst you are online, they would find……nothing. The hacker would probably then get bored and never bother you again.

So how do you create an anonymous PC? There are a few simple steps and rules to follow:

- Disable anything that records your activity. If using MS Internet Explorer turn off the cookies, clean out the history folders, and routinely remove cached files.
- Use removable storage media to save any downloaded files to.
- Only use your Internet PC for surfing. Do not use the word processor for business or personal letters.
- Make sure all your connection details are anonymous.
- Ensure the set up of your system is as standard as possible.
- Do not use your ISP Email for anything other than anonymous traffic.
- These few simple steps should help to keep your system clean and anonymous to the casual hacker.

Do not leave a footprint

When you surf the Internet you cannot fail to leave a footprint. A footprint is an electronic signature that identifies you as a unique identity on the Internet during your current session. Most ISPs now issue a new signature to you each time you log on to surf. But while you are surfing during a session after log on, every site you visit retains your electronic signature. If you are trying to find information on a sensitive subject it is possible to carry out an analysis of the sites you visit and the subjects you are searching for. It would be sensible to log off and on again a number of times during a sensitive search.

Although an ISP may provide you with a new signature, part of that signature will identify the ISP. If your organisation is large and has its own ISP this will identify your organisation. It is always better to go through a civilian ISP whenever possible.

It is possible to use a number of different ISPs. These days there are a huge number of free ISPs available. Each country has its own list of free ISPs and details of these can be obtained via the Internet. It is possible to hide the country from which you are searching from by dialling up an ISP in another country and beginning your search from there. It is almost impossible for a hacker to identify which country your call originated from because Telecom companies take their security very seriously. There is one thing that may identify your country of origin and that is the date and time of your search. When you surf the date and time of your PC is stamped on the search as part of the electronic signature. If this does not match your ISP time it may indicate that you are trying to hide something, so make sure your PCs time is set to the time zone of the country of the ISP you are using.

Traffic analysis

Every web site has the capability to log the number of visitors to its site and the electronic signature of the visitor. While you may be able to hide your identity, you cannot hide the fact that you have visited the site. If the number of visitors to a significant site increases dramatically then this may be an indicator that there is new or renewed

interest in the subject of the site. Such a site may be set up deliberately to identify interest, for example an obscure terrorist related site. The way to combat this is to ensure that trained personnel, in a central location, do all sensitive searches. This will ensure that searches are done quickly and without repetition. The security education of all personnel who have access to the Internet is also a very important factor.

Contact with others

There may be occasions when you want to communicate with others to solicit information. In most cases it is beneficial to explain who you are and ask for help or information. There may be other occasions when you will not want others to know exactly who you are or who you work for. The reasons for this must be decided case by case. It is reasonably easy to create an anonymous persona on the Web but the following points should be noted.

First, it is better to employ discretion rather than deception when soliciting information on the Web. This will be less publicly embarrassing later and will make an explanation of your action more reasonable.

Second, an anonymous persona should only be used for occasional requests for information. Any development of a relationship using the Internet should be discouraged. This is the field of other specialists, typically in the realm of HUMINT. Without proper control, such practices can lead to embarrassment.

Conclusions

- It is better to be discrete when searching on the Internet rather than employ deception.
- When searching discretely you are hiding your intentions.
- Practical measures should by applied sparingly and only with good reason.

CHAPTER IV: PROCESSING

Section A: Source Evaluation

Critically Analysing Information Sources

You can begin evaluating a physical information source (a book or an article for instance) even before you have the physical item in hand. Appraise a source by first examining the bibliographic citation. The bibliographic citation is the written description of a book, journal article, essay, or some other published material that appears in a catalog or index. Bibliographic citations characteristically have three main components: author, title, and publication information. These components can help you determine the usefulness of this source for your paper. (In the same way, you can appraise a web site by examining the home page carefully.)

a. Initial Appraisal

Author

1. What are the author's credentials--institutional affiliation (where he or she works), educational background, past writings, or experience? Is the book or article written on a topic in the author's area of expertise? You can use the various *Who's Who* publications for the U.S. and other countries and for specific subjects and the biographical information located in the publication itself to help determine the author's affiliation and credentials.

2. Have you seen the author's name cited in other sources or bibliographies? Respected authors are cited frequently by other scholars. For this reason, always note those names that appear in many different sources.

3. Is the author associated with a reputable institution or organization? What are the basic values or goals of the organization or institution?

Date of Publication

1. When was the source published? This date is often located on the face of the title page below the name of the publisher. If it is not there, look for the copyright date on the reverse of the title page. On web pages, the date of the last revision is usually at the bottom of the home page, sometimes every page.

2. Is the source current or out-of-date for your topic? Topic areas of continuing and rapid development, such as the sciences, demand more current information. On the other hand, topics in the humanities often require material that was written many years ago. At the other extreme, some news sources on the web now note the hour and minute that articles are posted on their site.

Edition or Revision

Is this a first edition of this publication? Further editions indicate a source has been revised and updated to reflect changes in knowledge, include omissions, and harmonize with its intended reader's needs. Also, many printings or editions may indicate that the work has become a standard source in the area and is reliable. If you are using a web source, do the pages indicate revision dates?

Publisher

Note the publisher. If the source is published by a university press, it is likely to be scholarly. Although the fact that the publisher is reputable does not necessarily guarantee quality, it does show that the publisher may have high regard for the source being published.

Title of Journal

Is this a scholarly or a popular journal? This distinction is important because it indicates different levels of complexity in conveying ideas. Or you may wish to check your journal title in the latest edition of *Katz's Magazines for Libraries* for a brief evaluative description.

b. Content Analysis

Having made an initial appraisal, you should now examine the body of the source. Read the preface to determine the author's intentions for the book. Scan the table of contents and the index to get a broad overview of the material it covers. Note whether bibliographies are included. Read the chapters that specifically address your topic. Scanning the table of contents of a journal or magazine issue is also useful. As with books, the presence and quality of a bibliography at the end of the article may reflect the care with which the authors have prepared their work.

Intended Audience

What type of audience is the author addressing? Is the publication aimed at a specialized or a general audience? Is this source too elementary, too technical, too advanced, or just right for your needs?

Objective Reasoning

Is the information covered fact, opinion, or propaganda? It is not always easy to separate fact from opinion. Facts can usually be verified; opinions, though they may be based on factual information, evolve from the interpretation of facts. Skilled writers can make you think their interpretations are facts.

Does the information appear to be valid and well researched, or is it questionable and unsupported by evidence? Assumptions should be reasonable. Note errors or omissions.

Are the ideas and arguments advanced more or less in line with other works you have read on the same topic? The more radically an author departs from the views of others in the same field, the more carefully and critically you should scrutinize his or her ideas.

Is the author's point of view objective and impartial? Is the language free of emotion-arousing words and bias?

Coverage

Does the work update other sources, substantiate other materials you have read, or add new information? Does it extensively or marginally cover your topic? You should explore enough sources to obtain a variety of viewpoints.

Is the material primary or secondary in nature? Primary sources are the raw material of the research process. Secondary sources are based on primary sources. For example, if you were researching Konrad Adenauer's role in rebuilding West Germany after World War II, Adenauer's own writings would be one of many primary sources available on this topic. Others might include relevant government documents and contemporary German newspaper articles. Scholars use this primary material to help generate historical interpretations--a secondary source. Books, encyclopaedia articles, and scholarly journal articles about Adenauer's role are considered secondary sources. In the sciences, journal articles and conference proceedings written by experimenters reporting the results of their research are primary documents. Choose both primary and secondary sources when you have the opportunity.

Writing Style

Is the publication organized logically? Are the main points clearly presented? Do you find the text easy to read, or is it stilted or choppy? Is the author's argument repetitive?

Evaluative Reviews

Locate critical reviews of books in a reviewing source, such as *Book Review Index*, *Book Review Digest,* or *Periodical Abstracts*. Is the review positive? Is the book under review considered a valuable contribution to the field? Does the reviewer mention other books that might be better? If so, locate these sources for more information on your topic.

Do the various reviewers agree on the value or attributes of the book or has it aroused controversy among the critics?

Source: http://www.library.cornell.edu/okuref/research/skill26.htm - LinkAuthor

Determining the Source of Web Pages

Step 1: Study the URL



The URL of every web page is displayed at the top of your web browser. Get into the habit of always reading the URL first before looking at the web page. (see How to Read a URL immediately following this section). Often times you have arrived directly at a web page via a search result or another hyperlink. You may be several levels "deep" in a particular web site. Study the URL and determine what kind of web server the page is hosted within. For example, delete the latter half of the URL and visit the main page at "computer.domain.name"

- If "company.domain.name" looks to be an Internet provider, or web hosting service, then the specific web page you were viewing probably belongs to a user of that service. At this point, your focus is strictly on the individual user. Go back to the URL and see of there is a logical breaking point in the URL. For example: **http://company.domain.name/pathname/filename.ext** can be shortened to **http://company.domain.name/pathname** If Pathname is a User_ID_NAME, then this approach should bring you to home page for a users' directory.
- If "company.domain.name" is some kind of specific organization that you want to learn more about, then proceed to the next steps.

Step 2: Do a "whois" on the domain name

All domain names on the Internet are registered with "domain name registrars" Domain name registrars are entities, which have been allocated the authority to register names for a specific subset of domain names. Most domain name registrars provide a "whois" function, where you can ask "whois domain.name" and they will tell you who has registered that domain name.

Useful Whois locations include:

- NSI Registry. Integrated database for all .com, .net, .org, .edu).
- Popular registrar's whois: Network Solutions, Register.com, and many other registrars.
- *AllWHOIS* (- Another nicely done integrated WHOIS interface to most WHOIS servers worldwide.

- Whowhizz - allows domain name look-ups of many countries.
- *Geektools* - provides a whois interface that will automatically query the right registrar - very useful when dealing with many types of international domain names.
- Whois.net - you can do a key-word search of domain names, with the results linking to whois.
- An extensive table of domain name registrars around the world is available at http://www.norid.no/domreg.html. Two letter country codes can also be found at the same site.
- US .MIL Domains can be researched at http://www.nic.mil/dodnic/
- Domainwatch -has some nice features, but seems to work for only some .com, .net, and .org names. Whois data records are linked to other search results such as: traceroute, map info, and list of all websites that link to the queried domain.
- Betterwhois - search the shared registry first and then the specific registrar.
- Network-tools.com. - integrates many functions into one page.
- Domainsurfer and Netcraft - Perform a keyword search against all domain names. This is helpful when searching for a new unique domain name.

Regional Internet registries handle the allocation of IP Numbers. Using their "whois" you can search 'based on IP Numbers, autonomous system numbers (ASNs), network-related handles, and other related Points of Contact (POCs)

- ARIN Whois - American Registry for Internet numbers.
- Ripe Whois - European IP network Coordination Center
- APNIC Whois - Asia Pacific Network Information Centre

To learn more about Domain Name structure and to locate domain name registrars for 2-letter domains (.UK, .JP, etc) explore the following links:

- Domain Name Registration (RFC 1591 - Domain Name System Structure and Delegation – on-line at http://www.isi.edu/in-notes/rfc1591.txt)
- Another list of Internet registrars from around the world (includes name, addresses and phone numbers) can be found at http://www.itu.int/net/cctlds/icc-a-z.htm.
- The US Department of Defense Network Information Centre (DoD NIC) manages the .mil generic Top Level Domain (gTDL): http://www.nic.mil/.
- The Internet Corporation for Assigned Names and Numbers (ICANN – http://www.ican.org/) will now have responsibility for the IP address space

allocation, protocol parameter assignment, domain name system management, and root server system.

- An excellent primer on Domain Name System (DNS) is can be found in Chapter 2 of DNS and BIND, 3rd Edition by O'Reilly & Associates. This book is also available on line at http://www.oreilly.com/catalog/dns3/chapter/ch02.html.
- A very comprehensive, yet layman friendly explanation of DNS is found "DNS - The Internet's Directory Service" on the Networking Next web site at http://www.networkingnext.com/basicnetworking/dns.html.

Source: http://navigators.com/whois.html

Step 3: Perform a Traceroute to the host name

Knowing who owns the domain may not satisfy your curiosity. You may also be interested in **where** is the web server located, and **how** is it connected to the Internet. There is a network utility called Traceroute, which is often used to trouble shoot network connections. In a Unix or Windows environment, Traceroute can be used to determine the specific network route taken from your workstation to reach a specific remote host. (Dos command is: "tracert sitename.com") Fortunately, there are many Unix systems on the Internet that allow us to originate a Traceroute from their location to any other location that you specify. You should recognize that a web server does NOT have to be hosted at an organization's location, but may be hosted with some Internet provider.

Step 4: Read the web-page and follow-up with the point of contact (if any)

Many webpages include point of contact information. You can also send an email to the page owner and ask, "Who are you". You should also examine the HTML Source code of the web pages - Many web-authoring programs include the author's name within meta_tags, which are included near the beginning of a web page. You may also learn about the organization by searching for that organization's name/domain name in message archives such as Google Groups (http://groups.google.com/).

Finally, if none of these approaches reveal any information about the web page/site... then you will want to "search upstream" of the web page to see who else links **towards** the web page you are interested in. (Explained in Annex A – More information on Source Evaluation)

Source: http://navigators.com/sesseval.html

How to Read a URL

URL's typically have the following format:



1. "**protocol://**" - This defines what Internet protocol is required to reach the online resource. Commonly used protocols include:
 - http:// - Hypertext Transfer Protocol - used to access a server that is supporting the WWW protocol (i.e. web server) - commonly used for downloading web pages and associated imbedded elements
 - ftp:// - File Transfer Protocol - used to download a file from a server supporting the FTP Protocol - commonly used to download a software program
 - news: - Used to access a Usenet newsgroup from your news server - Your web browser must be configured to access a specific news-server
 - telnet:// - Establish a telnet session (terminal emulation) to the specified host (often a VT100 Session)
 - mailto: Initiates an outgoing email message to the address specified
2. "**computer.domain.name**" - The domain name of the server where the information is located (can also be the server's IP number)
3. "**/pathname/**" - Usually consists of directory/subdirectory names. This defines where on the server's hard disk to look for the information.
4. **"filename.ext"** - The name of the desired file. If no specific filename is indicated, a file called "index.html", "default.html", or "home.html" may be downloaded if present. The ".ext" file extension cues the web browser on how to handle the downloaded file. The web browser can display some file-types within the browser display area, or it may invoke additional software such as a "plug-in" or external "helper application" to handle the file. Common file extension names include: ·
 - html, htm - Hypertext Mark-up Language (a web page) ·
 - gif, jpeg, tiff - A picture ·
 - wav, au, aif - A sound file ·
 - mov, avi, mpg, qt - a video clip ·
 - exe - An executable program for DOS/Windows (might be a self extracting archive) ·

- zip - A compressed archive based on PKzip (commonly used for DOS/Windows) ·
- hqx - A file that has been "binhexed" (commonly used for Macintosh archives)

Importance of Reading URL's. As you access online information resources from all over the Internet, it is important to read the URL of the displayed information (This information is displayed near the top of the web browser). The URL may be able to help you judge the value of the information. Consider the following examples:

1. Which web page would you use to influence your business unit's strategic plan?
 - http://www.sec.gov/rulings/exchanges/regulations.html
 - http://party.college.edu/freshman/joe/trading_regs.html
2. Which software program would you like to download?
 - ftp://ftp.microsoft.com/software/patches/fixit.exe
 - ftp://ftp.hackers.com/do/you/feel/lucky/trustme.exe
3. Which site is the US White House's official web site?
 - http://www.whitehouse.com
 - http://www.whitehouse.gov

The first two examples contain fictional URL's, which clearly illustrate the variety of resources you may encounter. The last example contains actual URL's, which show that URL's are not always a guarantee of authenticity. The first site is actually that of a commercial pornographic web site whereas the second is an official US government web site.

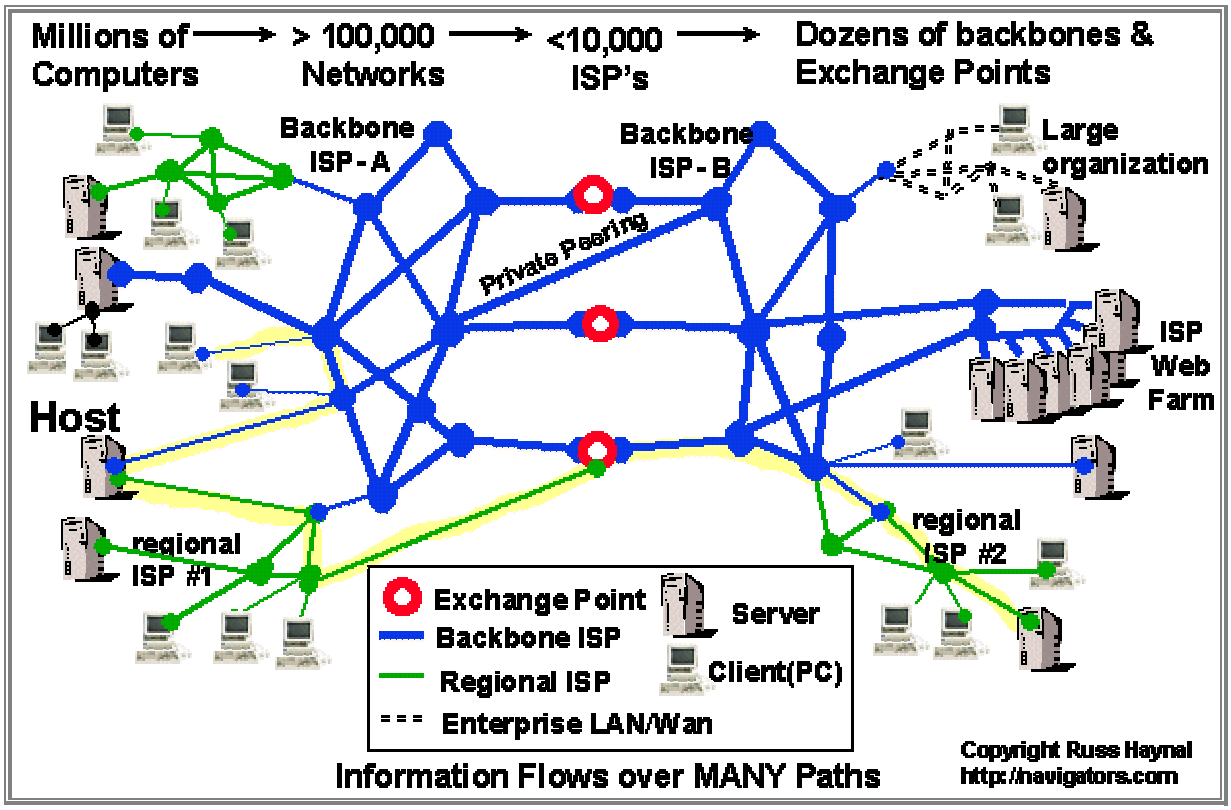
Tip: You should get into the habit of reading the URL of every web page before you even glance at the web page. URL's can also be used to decide which hyperlinks to select. While positioning your cursor over a hyperlink, the web browser will display (in the feedback area) the URL associated with the Hyperlink. This is a good way to "look before you leap"

Source: http://navigators.com/url.html

Traceroute

Using the *whois* function, you can determine the registered owner of a domain name. However, knowing who owns the domain may not satisfy your information requirement as ownership of a domain name is often less important than *where* the web server is physically located and *how* is it connected to the Internet. There is a network utility

called *traceroute*, which is often used to troubleshoot network connections. In a Unix or Windows environment, *traceroute* can be used to determine the specific network route taken from your workstation to reach a specific remote host. (Dos command: **tracertsitename.com**) Even more useful are the many Unix systems on the Internet that allow you to originate a traceroute from their location to any other location that you specify. Look at the following example of a *traceroute*.



Perform a traceroute to the host name

Look at this sample traceroute from http://www.boardwatch.com/to http://www.whitehouse.gov/:

1. t1 (204.144.169.2) 1.499 ms
2. t1.esoft.com (199.45.143.14) 9.549 ms
3. border-from-14-esoft.boulder.co.coop.net (199.45.130.13) 15.155 ms
4. core-gw-eth-0-2.boulder.co.coop.net (199.45.132.33) 33.277 ms
5. denver-cr2.bbnplanet.net (4.0.212.249) 19.309 ms
6. denver-br1.bbnplanet.net (4.0.52.1) 19.306 ms

7. oakland-br1.bbnplanet.net (4.0.1.133) 48.046 ms
8. oakland-br2.bbnplanet.net (4.0.1.78) 48.913 ms
9. sanjose1-br1.bbnplanet.net (4.0.1.74) 53.034 ms
10. mae-west2.us.psi.net (198.32.184.23) 47.213 ms
11. se.sc.psi.net (38.1.3.5) 148.414 ms
12. rc5.southeast.us.psi.net (38.1.25.5) 127.893 ms
13. ip2.ci3.herndon.va.us.psi.net (38.25.11.2) 139.433 ms
14. 198.137.240.33 (198.137.240.33) 134.218 ms
15. www2.whitehouse.gov (198.137.240.92) 141.93 ms

In the example, *boardwatch* gets its connectivity from "esoft.com" who get its connectivity from "coop.net" who is connected to BBNplanet (a backbone provider). BBNplanet Inter-connects with another backbone provider (PSI) through the MAE-West Connection point. It then appears that the whitehouse.gov web site is connected though PSI near Virginia. Recognize that an organization's website may not be located at the organization. The organization's website may be hosted someplace else. A more accurate approach to determine the location of the organization might be to do a traceroute to the organization's mailhost or proxy server.

Helpful information in reading *traceroute* results:

- Each Internet provider has their own naming convention. Most *traceroutes* travel across the largest Internet providers. A list of these as well as other helpful ISP-related information can be found on Russ Haynal's ISP page - http://navigators.com/isp.html.
- ISP node names may include an exchange point (MAE, NAP, PAIX). A list of the major exchange points can also be found on Haynal's ISP page - http://navigators.com/isp.html - naps
- ISP node names may describe the infrastructure topology (T1, T3, FDDI, ATM, HSSI, ETH)
- ISP node names may be the 3-letter code of the nearest airport in their node names. Here a list of all airport and city codes can be found at the following site - http://www.airportcitycodes.com/aaa/CCDBFrame.html.
- ISP node names may be just an IP Number. If you are trying to "read" the IP numbers, you should first understand how IP addressing works, how IP numbers are assigned, and then browse an IP network index. See the Internet Assigned Numbers Authority (http://www.iana.org) for information on IP addressing. There are several IP network indexes, the IP Network Index hosted by

dragonstar.net is one such IP network index - http://www.crackinguniversity2000.it/Ipindex/

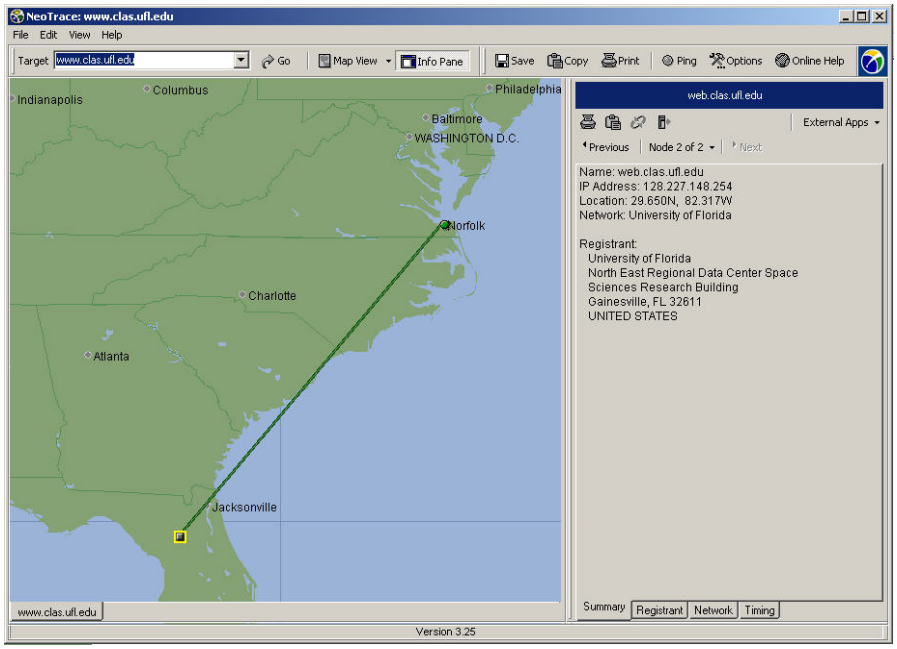
Traceroute Utilities:

You can perform *traceroutes* from various sites including: http://www.traceroute.org, http://www.geektools.com/traceroute.html, the Club Traceroute web page contains links to many *traceroute* resources and is found at http://www.amazing.com/Internet/club-traceroute.html.

Source: http://navigators.com/traceroute.html.

McAfee Visual Trace

A very convenient *traceroute* utility. McAfee acquired NeoTrace (shown below) and began to market an updated version under its new name. Visual Trace displays the traceroute nodes as symbols with country flags. Visual Trace also associates the *Whois* for each network node in the trace. More information at http://www.mcafee.com/myapps/mvt.



You may also want to download *Visual Route*, which can overlay your traced route over a geographic map (http://www.visualroute.com/). A Java-based version of Visual Route is available online through this web page: http://visualroute.datametrics.com/

Another useful utility is the Hostname to Latitude/Longitude Converter which can be accessed through this web page: http://cello.cs.uiuc.edu/cgi-bin/slamm/ip2ll/. This utility not only provides the Latitude and Longitude for the server in question, but it also plots the location on a map.

Traceroute is only one, albeit important tool in analysing the source of information found on the Internet. One final point to remember is that it is important to realize that a website can be hosted anywhere despite where it might logically seem to be located. Organizations make the decision as to where they want to host a web site. Sometimes they have the resources and personnel to host the web site at their own facility, but it is also common for an organization to host their site at a commercial web hosting facility. For example, the Tico Times is a newspaper from Costa Rica (http://www.ticotimes.co.cr/), yet a traceroute reveals that the web site is physically hosted in Pittsburgh, Pennsylvania.

Section B: Evaluation Checklists

The following section contains a series of checklists, which can be used in the evaluation of various types of web pages. Virtually all web sources can be categorized under the following headings:

- Advocacy
- Business/Marketing
- News
- Information
- Personal

While not intended to be exhaustive, they provide a useful framework when evaluating web pages. Readers are encouraged to add their own steps based on their experience as they see fit. Note that in all of these cases the greater number of questions listed below answered ***"yes"***, the more likely one is able to determine whether the source is of high information quality.

Evaluation Checklist for an Advocacy Web Page

An **Advocacy Web Page** is one sponsored by an organization attempting to influence public opinion (that is, one trying to sell ideas). The URL address of the page frequently ends in **.org** (organization). **Examples:** Bellona Foundation (http://www.bellona.org/), Human Rights Watch (http://www.humanrightswatch.org/), and Amnesty International (http://www.amnesty.org/).

Criterion #1: AUTHORITY

1. **Is it clear what organization is responsible for the contents of the page?**
2. Is there a link to a page describing the goals of the organization?
3. **Is there a way of verifying the legitimacy of this organization? That is, is there a phone number or postal address to contact for more information? (Simply an email address is not enough.)**
4. Is there a statement that the content of the page has the official approval of the organization?
5. Is it clear whether this is a page from the national or local chapter of the organization?
6. Is there a statement giving the organization's name as copyright holder?

Criterion #2: ACCURACY

1. Are the sources for any factual information clearly listed so they can be verified in another source? (If not, the page may still be useful to you as an example of the ideas of the organization, but it is not useful as a source of factual information).
2. Is the information free of grammatical, spelling, and typographical errors? (These kinds of errors not only indicate a lack of quality control, but can actually produce inaccuracies in information.)

Criterion #3: OBJECTIVITY

1. Are the organization's biases clearly stated?
2. If there is any advertising on the page, is it clearly differentiated from the informational content?

Criterion #4: CURRENCY

1. Are there dates on the page to indicate:
 a. When the page was written?
 b. When the page was first placed on the web?
 c. When the page was last revised?
2. Are there any other indications that the material is kept current?

Criterion #5: COVERAGE

1. Is there an indication that the page has been completed, and is not still under construction?
2. Is it clear what topics the page intends to address?
3. Does the page succeed in addressing these topics, or has something significant been left out?
4. Is the point of view of the organization presented in a clear manner with its arguments well supported?

Source: http://www2.widener.edu/Wolfgram-Memorial-Library/webevaluation/advoc.htm

Evaluation Checklist for a Business/Marketing Web Page

A **Business/Marketing Web Page** is one sponsored by a commercial enterprise (usually it is a page trying to promote or sell products). The URL address of the page frequently ends in **.com** (commercial). **Examples:** Microsoft Inc. (http://www.microsoft.com/), DaimlerChrysler AG (http://www.daimlerchrysler.com/), as well as millions of other large and small companies using the web for business purposes.

Criterion #1: AUTHORITY

1. **Is it clear what company is responsible for the contents of the page?**
2. Is there a link to a page describing the nature of the company, who owns the company, and the types of products the company sells?
3. **Is there a way of verifying the legitimacy of this company? That is, is there a phone number or postal address to contact for more information? (Simply an email address is not enough.)**
4. Is there a way of determining the stability of this company?
5. Is there a statement that the content of the page has the official approval of the company?
6. Is there a statement giving the company's name as copyright holder?

Criterion #2: ACCURACY

1. Has the company provided a link to outside sources such as product reviews or reports filed with the SEC (the Securities and Exchange Commission) which can be used to verify company claims?
2. Are the sources for any factual information clearly listed so they can be verified in another source?
3. Is the information free of grammatical, spelling, and typographical errors? (These kinds of errors not only indicate a lack of quality control, but can actually produce inaccuracies in information.)

Criterion #3: OBJECTIVITY

1. For any given piece of information, is it clear what the company's motivation is for providing it?
2. If there is any advertising on the page, is it clearly differentiated from the informational content?

Criterion #4: CURRENCY

1. Are there dates on the page to indicate:
 a. When the page was written?
 b. When the page was first placed on the web?
 c. When the page was last revised?
2. Are there any other indications that the material is kept current?
3. For financial information, is there an indication it was filed with the SEC and is the filing date listed? For material from the company's annual report, is the date of the report listed?

Criterion #5: COVERAGE

1. Is there an indication that the page has been completed, and is not still under construction?
2. If describing a product, does the page include an adequately detailed description of the product?
3. Are all of the company's products described with an adequate level of detail?
4. Is the same level of information provided for all sections or divisions of the company?

Evaluation Checklist for a News Web Page

A **News Web Page** is one whose primary purpose is to provide extremely current information. Many international news outlets have web pages whose URL address of the page ends in **.com** (commercial), though many national news outlets web pages end in their respective nation's country code. One excellent example of this is the web page for BBC News – http://news.bbc.co.uk/. Other examples of news web pages are CNN (http://www.cnn.com/), Reuters (http://www.reuters.com/), and Agence France-Presse (http://www.afp.com/).

Criterion #1: AUTHORITY

1. **Is it clear what company or individual is responsible for the contents of the page?**
2. Is there a link to a page describing the goals of the company?
3. **Is there a way of verifying the legitimacy of the company? That is, is there a phone number or postal address to contact for more information? (Simply an email address is not enough.)**
4. Is there a non-web equivalent version of this material which would provide a way of verifying its legitimacy?
5. If the page contains an individual article, do you know who wrote the article and his or her qualifications for writing on this topic?
6. Is it clear who is ultimately responsible for the content of the material?
7. Is there a statement giving the company's name as copyright holder?

Criterion #2: ACCURACY

1. Are sources for factual information clearly listed so they can be verified in another source?
2. Are there editors monitoring the accuracy of the information being published?
3. Is the information free of grammatical, spelling, and typographical errors? (These kinds of errors not only indicate a lack of quality control, but can actually produce inaccuracies in information.)

Criterion #3: OBJECTIVITY

1. Is the informational content clearly separated from the advertising and opinion content?
2. Are the editorials and opinion pieces clearly labelled?

Criterion #4: CURRENCY

1. Is there a link to an informational page which describes how frequently the material is updated?
2. Is there an indication of when the page was last updated?
3. Is there a date on the page to indicate when the page was placed on the web?
 a. If a newspaper, does it indicate what edition of the paper the page belongs to?
 b. If a broadcast, does it indicate the date and time the information on the page was originally broadcast?

Criterion #5: COVERAGE

1. Is there a link to an informational page which describes the coverage of the source?
2. If you are evaluating a newspaper page and there is a print equivalent, is there an indication of whether the Web coverage is more or less extensive than the print version?

Evaluation Checklist for an Informational Web Page

An **Informational Web Page** is one whose purpose is to present factual information. The URL Address frequently ends in **.edu** or **.gov**, as many of these pages are sponsored by educational institutions or government agencies. **Examples:** dictionaries, thesauri, transportation schedules, calendars of events, and statistical data.

Criterion #1: AUTHORITY

1. **Is it clear who is responsible for the contents of the page?**
2. Is there a link to a page describing the purpose of the sponsoring organization?
3. **Is there a way of verifying the legitimacy of the page's sponsor? That is, is there a phone number or postal address to contact for more information?**
4. Is it clear who wrote the material and are the author's qualifications for writing on this topic clearly stated?
5. If the material is protected by copyright, is the name of the copyright holder given?

Criterion #2: ACCURACY

1. Are the sources for any factual information clearly listed so they can be verified in another source?
2. Is the information free of grammatical, spelling, and typographical errors? (These kinds of errors not only indicate a lack of quality control, but also can actually produce inaccuracies in information.)
3. Is it clear who has the ultimate responsibility for the accuracy of the content of the material?
4. If there are charts and/or graphs containing statistical data, are the charts and/or graphs clearly labelled and easy to read?

Criterion #3: OBJECTIVITY

1. Is the information provided as a public service?
2. Is the information free of advertising?
3. If there is any advertising on the page, is it clearly differentiated from the informational content?

Criterion #4: CURRENCY

1. Are there dates on the page to indicate:
 a. When the page was written?
 b. When the page was first placed on the web?
 c. When the page was last revised?
2. Are there any other indications that the material is kept current?
3. If material is presented in graphs and/or charts, is it clearly stated when the data was gathered?
4. If the information is published in different editions, is it clearly labelled what edition the page is from?

Criterion #5: COVERAGE

1. Is there an indication that the page has been completed, and is not still under construction?
2. Is there a clear indication of whether the entire work is available on the web or only parts of it?

Evaluation Checklist for a Personal Web Page

A **Personal Web Page** is one published by an individual who may or may not be affiliated with a larger institution. Although the URL address of the page may have a variety of endings (e.g. *.com, .edu*, etc.), a tilde (~) is frequently embedded somewhere in the URL. Some examples of personal web pages include Gary Capeci's web page – (http://www.gangland.com/), Julie's Astronomy Page (http://www.geocities.com/Astronomy30/), and The Missile Index (http://www.index.ne.jp/missile_e/index.html).

Criterion #1: AUTHORITY

1. **Is it clear what individual is responsible for the contents of the page?**
2. Does the individual responsible for the page indicate his or her qualifications for writing on this topic?
3. **Is there a way of verifying the legitimacy of this individual?** (Because it is difficult to verify the legitimacy of an individual, personal home pages may be a useful source for personal opinion but use extreme caution when using them as a source for factual information.)

Criterion #2: ACCURACY

1. Are the sources for any factual information clearly listed so they can be verified in another source? (If not, the page may still be useful to you as an example of the ideas of the individual, but it is not useful as a source of factual information.)
2. Is the information free of grammatical, spelling, and typographical errors? (These kinds of errors not only indicate a lack of quality control, but also can actually produce inaccuracies in information.)

Criterion #3: OBJECTIVITY

- Are the person's biases clearly stated?

Criterion #4: CURRENCY

1. Are there dates on the page to indicate:
 a. When the page was written?
 b. When the page was first placed on the web?
 c. When the page was last revised?
2. Are there any other indications that the material is kept current?

Criterion #5: COVERAGE

1. Is there an indication that the page has been completed, and is not still under construction?
2. If there is a print equivalent to the web page, is there a clear indication of whether the entire work is available on the web or only parts of it?

Source: http://www2.widener.edu/Wolfgram-Memorial-Library/webevaluation/perspg.htm

Section C: Validated Source Lists

Considerable effort is required to validate an Internet source. Industry leaders, once discovered and validated, may be realistically relied upon to maintain the same degree of accuracy and consistency in reporting. Other collateral sources must be continually validated to ensure their accuracy.

Many Internet users either fail to make the effort to validate information sources prior to using the information that they provide, or do not take steps to capture the source validation data that the evaluation process produces. Capturing this information allows the analyst to refer back to the source evaluation prior to returning to that source. Perhaps more importantly, it allows the analyst to share his sources with other collaborating analysts. Rather than simply providing a list of Internet hyperlinks, the inclusion of source evaluation data provides a broader understanding of the analytical judgements made in including a particular source while excluding another.

A number of options for maintaining and exchanging sources and source validation exist. A live web-page with hyperlinks directly to the source is an effective means with which to disseminate this data. Security can be achieved if this list is maintained behind a firewall or other protection protocol. Some organizations have used lists of sources arranged by subject and managed either in a spreadsheet or a text document.

Powermarks 3.5

The bookmark management program *Powermarks 3.5*[6] is a highly effective means with which to organize large amounts of Internet bookmarks as well as capture and maintain source evaluation data.

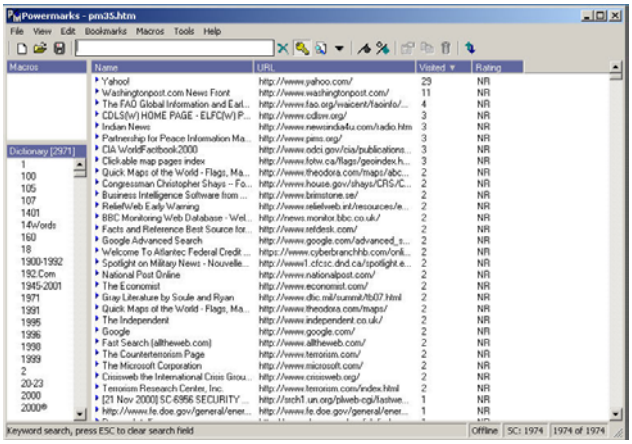
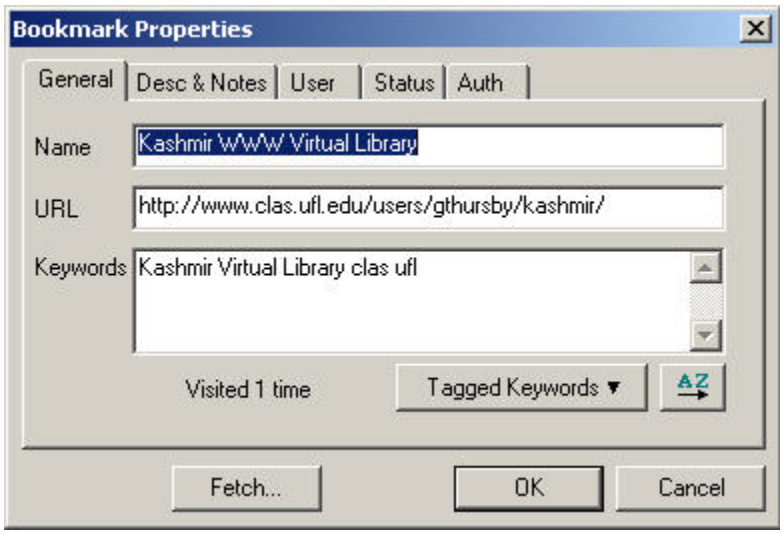


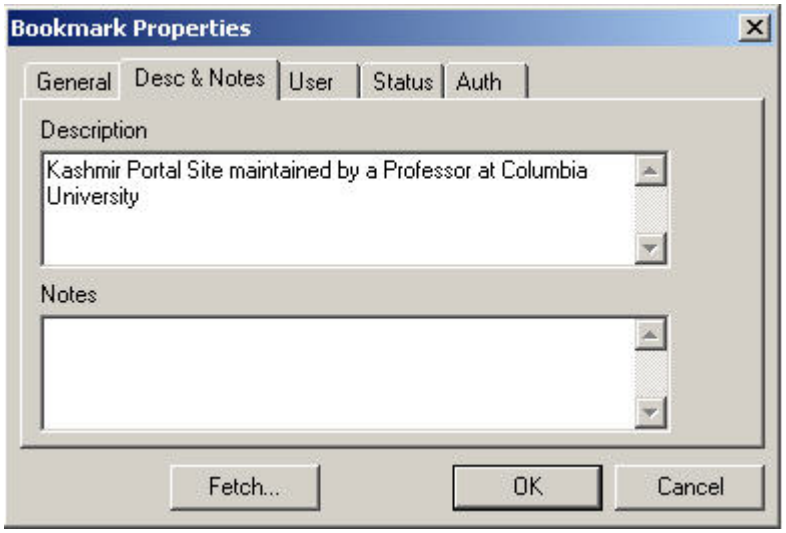
Figure 1 – Powermarks 3.5 Main Screen

[6] http://www.kaylon.com/power.html

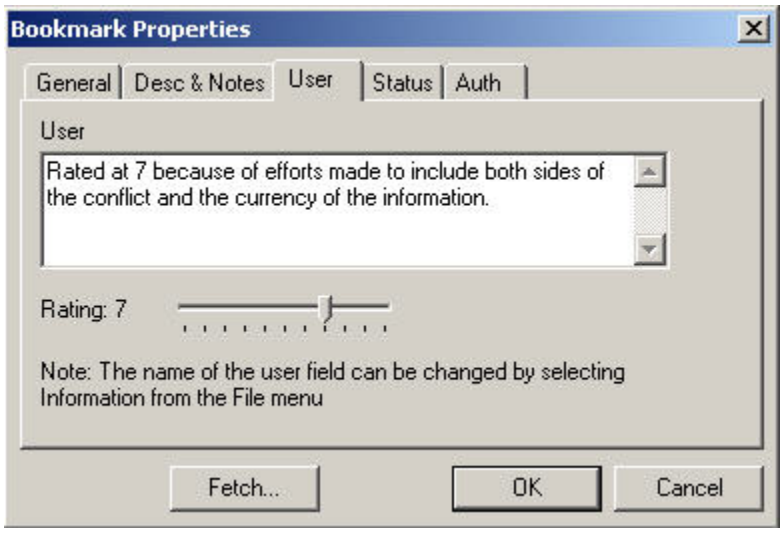
The traditional method of storing bookmarks has been in a hierarchical file structure by subject type. The main limitation of this method is that a particular link may have applicability across a number of subjects. The only means with which to provide that link with visibility across these topics was to store it in several places. Contrasting with that approach, Powermarks stores bookmarks in a flat file database that is searched by keyword.



When a link is saved, the properties screen opens and the analysts are able to list in the keywords field, all the relevant subjects related to that particular page. When retrieving a link, the Powermarks main screen opens with a search box that asks for keywords to be entered to retrieve links saved in the local database. This is a highly effective means with which to manage links that cut across traditional subject lines.



The description and notes field allow the analyst to identify the source in plain text with amplifying details. Rather than a link to the Internet, the source description can provide a sense of why it is important to an analyst.



The user-rating field provides the analyst with the means with which to attach a subjective rating of 1-10 to the site and the information that it provides. It also provides a text box to explain why the rating has been attached to the source.

Sources of known reliability can be used to corroborate new information sources. Source reliability is not static. It is affected by new biases, changes in funding sources, and personnel changes, among other factors. Sources should always be monitored closely for shifts in their reporting. The maintenance of accurate records is essential for tracking source consistency and identifying and monitoring new sources.

By maintaining an accurate source list, time can be saved in the collection of information from the Internet. While a number of methods for the maintenance of these records are available, commercially available solutions like Powermarks provide an effective, low-cost solution to the record maintenance problem.

While a server-based solution is not available for this particular product, it does have the means with which to export and import Powermarks files and to maintain its database on its corporate server for collaboration purposes.

Section D: Effective Summary

The combination of information browsers, word processors and the myriad information sources available via the Internet produces a highly tempting option for analysts to gather vast quantities of information on topics of interest. Even with disciplined collection strategies, information overload is an ever-present problem. While open sources can contribute to satisfying an information requirement in a timely fashion, the resulting information must be structured so as to be relevant to the analyst and easy to use and understand for others who receive it.

Effective summary is an important yet elementary skill necessary to shape large quantities of information into a manageable form. When gathering data for further dissemination, the inclusion of a summary paragraph that captures the essence of the information can be the difference between whether the information is reviewed or rejected.

Copernic Summarizer

The most effective means of summary is the application of analytical skill to information in order to capture the salient points relating to the stated information requirement. A number of commercial products are now being marketed to assist in the rapid summary of information sources. One is *Copernic Summarizer*[7].



Figure 2 – Complete Web-page 1200 words in length

[7] http://www.copernic.com/products/summarizer/

Copernic Summarizer can analyse text of any length, on any subject, in any one of four languages (English, French, German and Spanish), and create a summary as short or as long as you want it to be. It can summarize Word documents, Web pages, PDF files, e-mail messages and even text from the Clipboard.

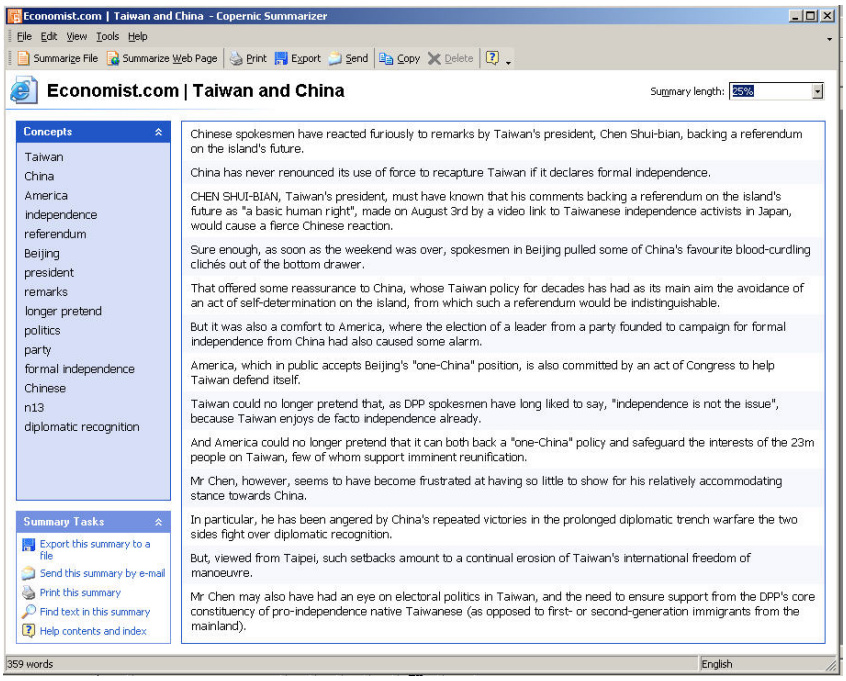


Figure 3 – Copernic Summarizer produced summary of previous article (25% of original length).

Summary reports include key concepts and key sentences according to the configuration of the software. It is possible to summarize a whole document or a selected part of the document. If the summary does not capture the essence of the topic, it is possible to refine the summary report by deleting selected concepts and sentences, with an automatic summary updating when a concept is deleted.

The resulting summary report may be exported in various file formats (HTML, XML, Rich Text Format and Text file) and appended to files. These files can be distributed by the integrated email function, printed, or copied into other documents.

While not a solution to the problem of information overload, the judicious use of these technologies can assist in the reduction of large documents to more manageable lengths.

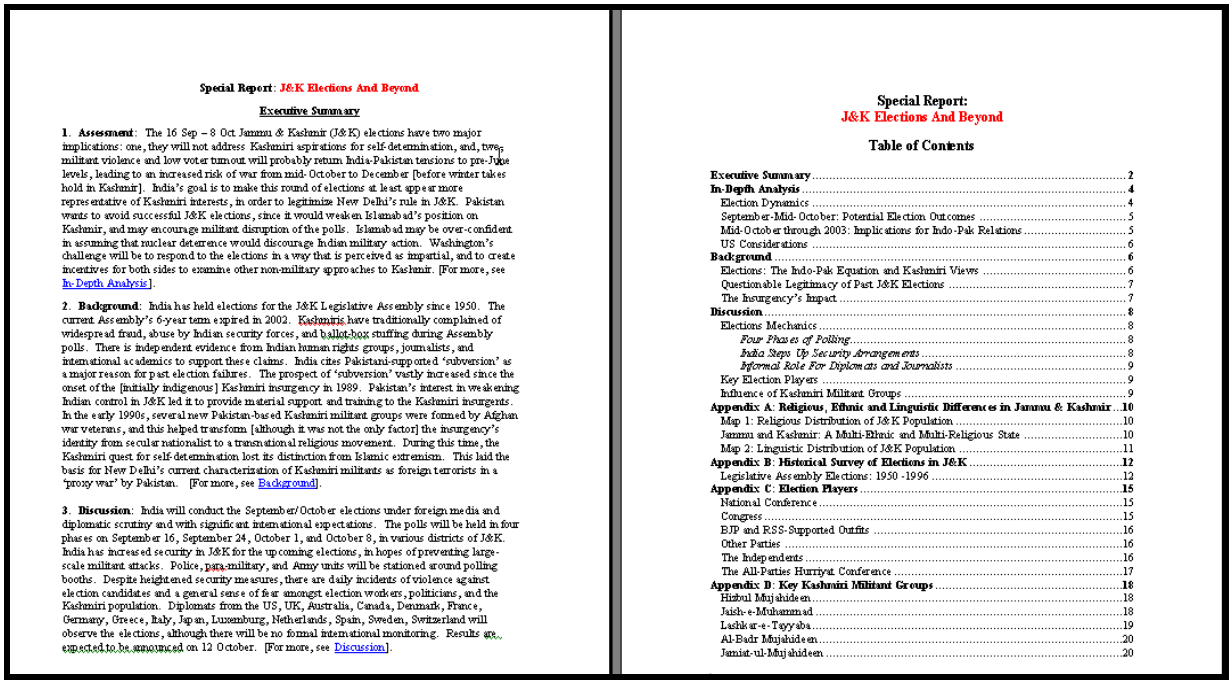
CHAPTER V: DISSEMINATION

The essential fundamentals of effective dissemination are four-fold: the right person must receive the right product at the right time and in the right format. While this principle is well accepted in classified intelligence disciplines, it is no less relevant for Internet-derived material. Given the ease with which material can be collected and collated from the Internet, its dissemination requires probably even greater care if it is not to further contribute to information overload.

Information provided must not only be accurate and relevant, but it must be structured and presented in such a way that the recipient can use it easily, assimilate it quickly, and understand its significance in time to act on it effectively. Since each level of command both within and outside an organization have differing information-detail and time-management requirements, intelligence and information support products must be structured, presented, and disseminated in ways that fit these varying requirements.

Section A: Report Layering

An effective means with which to present collated information is with a "layered" product. Through the use of an Executive Summary and a Table Of Contents, followed by only the relevant material, a product collected from Internet sources can simultaneously satisfy the information needs of a variety of users.



Special Report: J&K Elections And Beyond

Executive Summary

1. **Assessment**: The 16 Sep – 8 Oct Jammu & Kashmir (J&K) elections have two major implications: one, they will not address Kashmiri aspirations for self-determination, and, two, militant violence and low voter turnout will probably return India-Pakistan tensions to pre-June levels, leading to an increased risk of war from mid-October to December [before winter takes hold in Kashmir]. India's goal is to make this round of elections at least appear more representative of Kashmiri interests, in order to legitimize New Delhi's rule in J&K. Pakistan wants to avoid successful J&K elections, since it would weaken Islamabad's position on Kashmir, and may encourage militant disruption of the polls. Islamabad may be over-confident in assuming that nuclear deterrence would discourage Indian military action. Washington's challenge will be to respond to the elections in a way that is perceived as impartial, and to create incentives for both sides to examine other non-military approaches to Kashmir. [For more, see In-Depth Analysis].

2. **Background**: India has held elections for the J&K Legislative Assembly since 1950. The current Assembly's 6-year term expired in 2002. Kashmiris have traditionally complained of widespread fraud, abuse by Indian security forces, and ballot-box stuffing during Assembly polls. There is independent evidence from Indian human rights groups, journalists, and international academics to support these claims. India cites Pakistani-supported 'subversion' as a major reason for past election failures. The prospect of 'subversion' vastly increased since the onset of the [initially indigenous] Kashmiri insurgency in 1989. Pakistan's interest in weakening Indian control in J&K led it to provide material support and training to the Kashmiri insurgents. In the early 1990s, several new Pakistan-based Kashmiri militant groups were formed by Afghan war veterans, and this helped transform [although it was not the only factor] the insurgency's identity from secular nationalist to a transnational religious movement. During this time, the Kashmiri quest for self-determination lost its distinction from Islamic extremism. This laid the basis for New Delhi's current characterization of Kashmiri militants as foreign terrorists in a 'proxy war' by Pakistan. [For more, see Background].

3. **Discussion**: India will conduct the September/October elections under foreign media and diplomatic scrutiny and with significant international expectations. The polls will be held in four phases on September 16, September 24, October 1, and October 8, in various districts of J&K. India has increased security in J&K for the upcoming elections, in hopes of preventing large-scale militant attacks. Police, para-military, and Army units will be stationed around polling booths. Despite heightened security measures, there are daily incidents of violence against election candidates and a general sense of fear amongst election workers, politicians, and the Kashmiri population. Diplomats from the US, UK, Australia, Canada, Denmark, France, Germany, Greece, Italy, Japan, Luxemburg, Netherlands, Spain, Sweden, Switzerland will observe the elections, although there will be no formal international monitoring. Results are expected to be announced on 12 October. [For more, see Discussion].

Special Report:
J&K Elections And Beyond

Table of Contents

Executive Summary 2
In-Depth Analysis 4
Election Dynamics 4
September-Mid-October: Potential Election Outcomes 5
Mid-October through 2003: Implications for Indo-Pak Relations 5
US Considerations 6
Background 6
Elections: The Indo-Pak Equation and Kashmiri Views 6
Questionable Legitimacy of Past J&K Elections 7
The Insurgency's Impact 7
Discussion 8
Elections Mechanics 8
Four Phases of Polling 8
India Steps Up Security Arrangements 8
Informal Role For Diplomats and Journalists 9
Key Election Players 9
Influence of Kashmiri Militant Groups 9
Appendix A: Religious, Ethnic and Linguistic Differences in Jammu & Kashmir 10
Map 1: Religious Distribution of J&K Population 10
Jammu and Kashmir: A Multi-Ethnic and Multi-Religious State 10
Map 2: Linguistic Distribution of J&K Population 11
Appendix B: Historical Survey of Elections in J&K 12
Legislative Assembly Elections: 1950 -1996 12
Appendix C: Election Players 15
National Conference 15
Congress 15
BJP and RSS-Supported Outfits 16
Other Parties 16
The Independents 16
The All-Parties Hurriyat Conference 17
Appendix D: Key Kashmiri Militant Groups 18
Hizbul Mujahideen 18
Jaish-e-Muhammad 18
Lashkar-e-Tayyaba 19
Al-Badr Mujahideen 20
Jamiat-ul-Mujahideen 20

An approach in structuring information is to consider how those who receive it use information. A safe rule-of-thumb is the following:

- Executives (decision-makers) require executive summaries
- Staff officers require relatively complete summaries focused on their assigned areas with enough background for them to understand the "big picture"
- Analysts often need a detailed treatment of the subject within their assigned area of interest in order to make their own assessment of information reliability

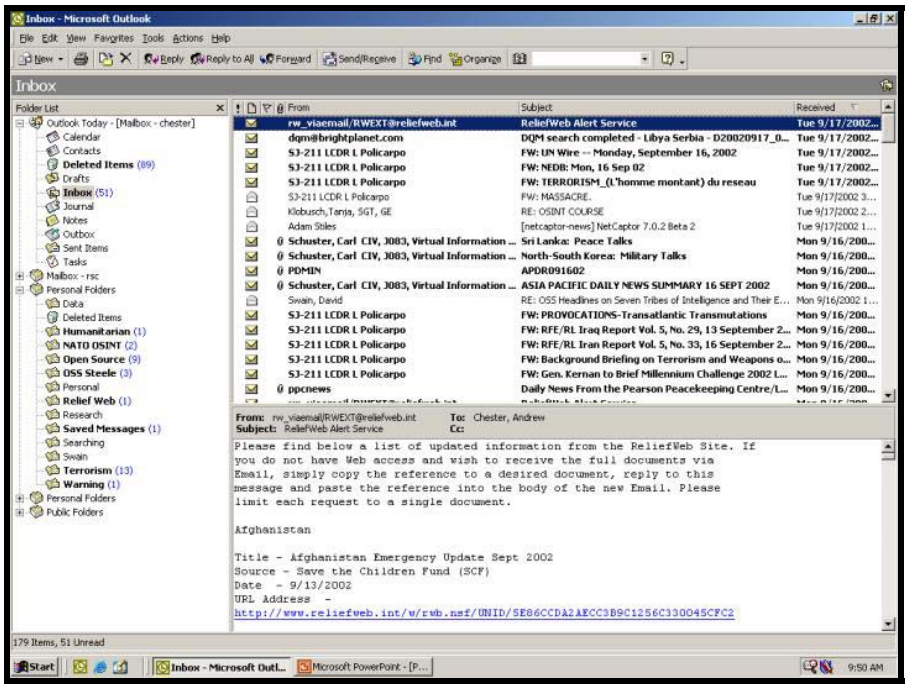
Section B: Dissemination with *Microsoft Outlook*

An alternate means of dissemination available to NATO Intelligence staffs is direct email of relevant collected material at the time of its collection. For particularly time-sensitive material, this may be appropriate. *Microsoft Outlook* is the email standard within NATO commands. This software supports distribution lists so that one researcher can collect material and disseminate it quickly to all staff members who are working on a subject. This is highly effective in an intelligence watch structure. A watch officer can be supported by dedicated open source analysts who are able to manage a mission-focused collection effort on their behalf.

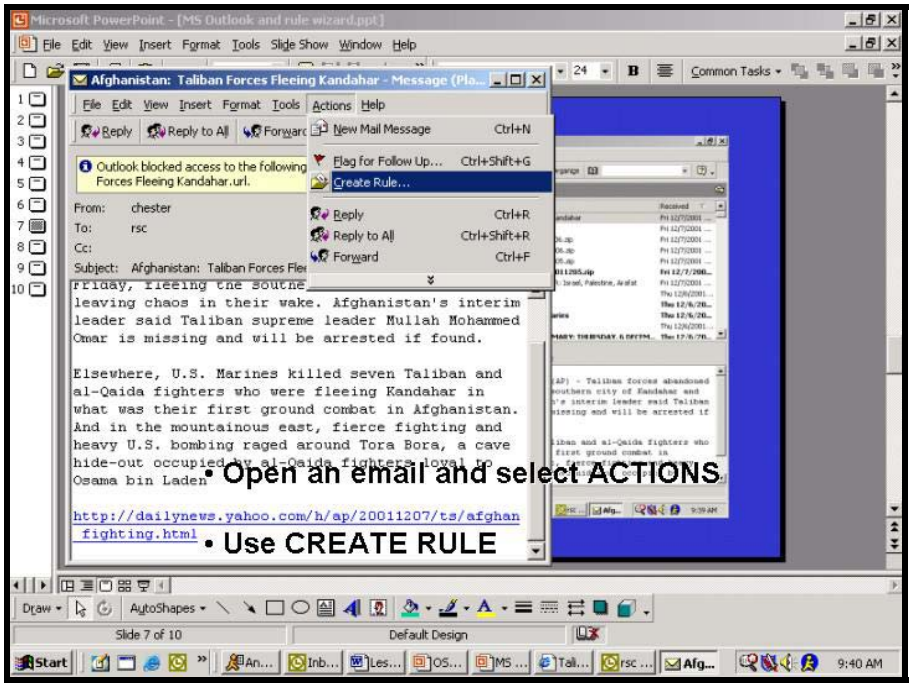
Some OSINT organizations disseminate vast amounts of material (several hundred messages daily) directly to a specific set of users through distribution lists. Unless the user is prepared to deal with a large flow of messages, the collected material quickly is treated as *SPAM* by its recipient. *Outlook* can help with this.

It is possible to use Outlook as a database for collected material placed either manually or automatically within separate folders. These folders can then be searched locally for collected material. Each user is able to establish a series of folders, which can be populated with relevant material collected from the Internet or sent to an email account by others.

Most *Outlook* users are familiar with folders; fewer understand how they can be automatically managed. The ***rules*** function in *Outlook* can be optimized to help mitigate the impact of a large volume of email.



The Rules Wizard can be used to automatically store files received within an email inbox based on criteria set by the user. Emails or copies of emails received from a particular email address or with a specific keyword in its title can automatically be placed into a file for later reference. This provides the recipient with the flexibility to either deal directly with the information as it is received or later when they are ready to conduct analysis on a specific topic.



Section C: Dissemination and Classification

Intelligence is classified to protect sources, methods and intentions. While information hosted by Internet sources is inherently unclassified, its collection in support of some mission objectives can make its retention or dissemination by an intelligence staff a sensitive issue. It is established intelligence doctrine that the originator of the information is responsible for its classification. This goes for material collected from the Internet as well.

Dangers arise when information gathered from the Internet is classified without good reason. Over-classification of any intelligence inhibits its effective dissemination. Once material collected from Internet sources is given any classification, its dissemination can only be achieved via classified systems. In some cases, this may limit the utility of the information particularly if its collection was intended to support a broader international effort outside the traditional military structure within NATO.

When information gathered from the Internet is merely reproduced within a classified intelligence product, confidence in the classification system is compromised. If an intelligence analyst can gather a particular item from an Internet source, it is likely that other members of the staff, equally interested in the subject, will be familiar with the source. Seeing Internet material merely repeated back under a classified banner undermines the intelligence process.

While in some cases it makes sense to protect the source, in most cases it does not. Information gathered from the Internet should be treated in a manner appropriate to the mission. For example, general information collected on the subject of terrorism in southern Europe would not expose any NATO plans or operations. Public statements by both military and political leaders within the Alliance have made clear NATO's interest in the field of terrorism. Even a compilation of relevant documents is unlikely to require protection with classified markings. However, specific collection of information from the Internet on the presence of terrorist cells or particular leaders in the Naples, Italy area would require greater protection both in the manner in which the information was gathered and in the steps taken to protect it.

One of the principal advantages that OSINT brings to the intelligence process is the ability to rapidly prepare intelligence products that can be easily shared with coalition partners. The use of open sources to construct an intelligence picture that closely mirrors the classified intelligence picture but that does not compromise sources and methods provides a commander and his intelligence staff with an important tool to support coalition warfare. NATO operations have historically been conducted in a multinational environment with NATO forces alongside those of non-NATO troop contributing nations providing the military component within a larger international effort. Reliable and sharable unclassified information enables the commander to benefit from information exchanges outside of his command structure. These information exchanges foster a common view of the operating area among all mission elements and nurtures an environment of information sharing within a coalition.

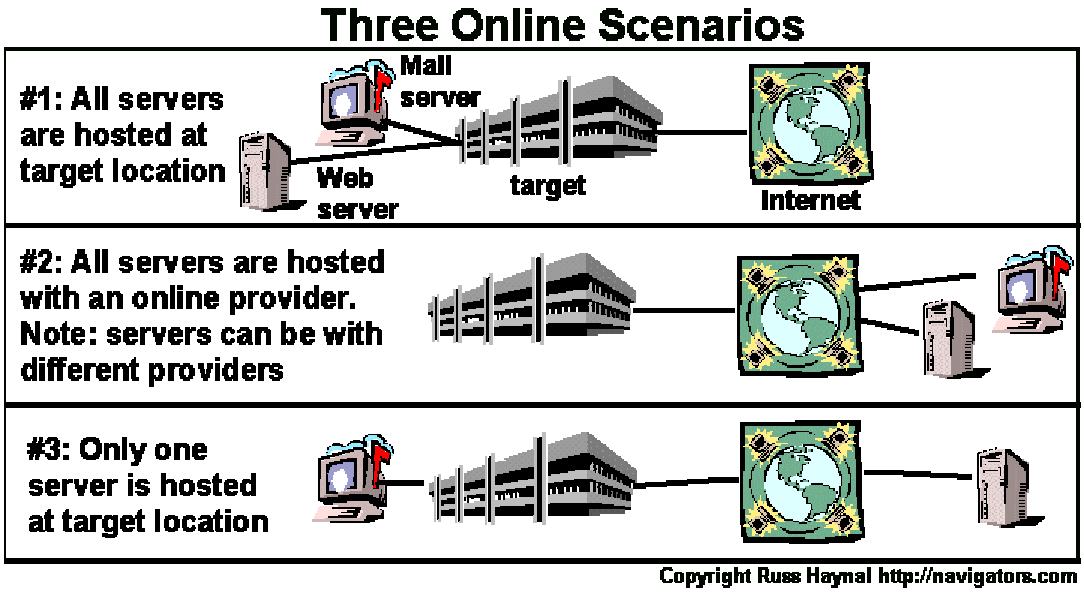
While there are always limitations to information sharing, at least a robust open source exploitation capability assures a minimal common appreciation of the situation including terrain and civil factors. This benefit crosses mission essential civil-military lines. However, a strict adherence to classifying all products that include intelligence staff in their preparation eliminates these potential advantages.

A final point on dissemination in a coalition environment is the concept of "bottom-up" report compilation. By beginning with unclassified sources, a report can be created on a subject that is instantly shareable with whomever the commander chooses. Given the broad range of information sources available today virtually any subject can initially be evaluated with open sources. After this initial process, relevant classified collateral reporting can be added to increase the intelligence value of the product. Ultimately, a variety of products can be created at various levels of classification to support mission requirements. This process contrasts sharply with the traditional approach of sanitizing/declassifying intelligence to support coalition partners. Yet, it is a faster process that both makes use of open sources to produce products for wide distribution and serves to integrate open source derived material directly into the classified intelligence production process.

Building intelligence products by the "bottom up" method provides a quick and efficient means of building products for multiple security domains and audiences without having to resort to a disclosure process.

ANNEXES:

Annex A: More information on Source Evaluation



Consider these scenarios:

1. The organization hosts all their servers at their own facility. A traceroute to the web server or email server will also indicate how the entire organization is connected

2. The organization chooses to host all of their servers with various out-sourced solutions. Recognize that the web server, email server, and Access provider to the organization's building can all be with different vendors. The most assured way of determining how this organization is connected would be to do a traceroute to a connection persona of one of the employees who has visited a web site (This method works for all scenarios).

3. Some servers may be out-sourced, some may be located locally. A traceroute to a locally hosted server will show how the organization is connected

Problem - How do you discover the server locations associated with a domain name? The Information is located online in the DNS Records for the domain. Just "ask" any domain name server for the DNS record of the target site. This information is widely used to properly route web requests and email messages to the domains servers wherever they may be located.

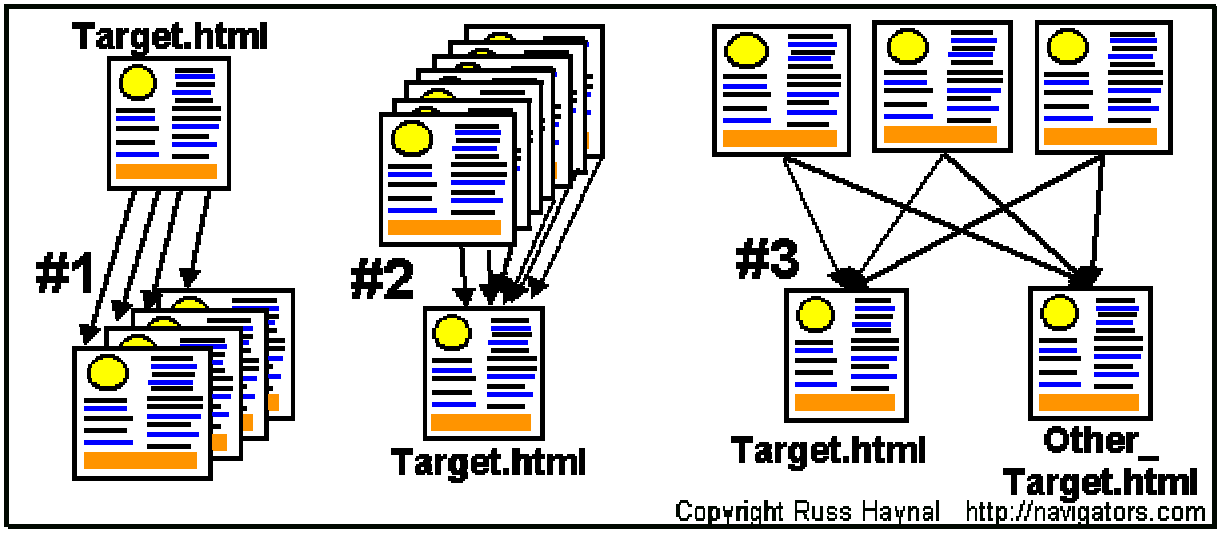
Here are several integrated multi-use tools:

- Network-tools.com (http://www.network-tools.com/) is another great resource (click on one of the numbers to go to a mirrored page) - Be sure to try **DNS Records**.
- Sam Spade (http://www.samspade.org/) tries the **scan rDNS** to scan a network block for named hosts.
- Codeflux (http://www.codeflux.com/tools) has easy interface to whois, dig, traceroute, etc.
- The multiple DNS look-up engine found here - http://www.bankes.com/nslookup.htm- allows you to enter a web domain, or IP number, and this site will allow you to discover who are the target's neighbours (from an IP number point of view)
- Zone Edit has a web-based DNS look-up that can be found here http://www.zoneedit.com/lookup.html

Searching Upstream

You've just found a great target web page. You've even followed the links "downstream" from that web page to other web pages.

Now do the most important search. Find the web pages that point **towards** the target web page (searching "upstream")



Look at these three scenarios and see the value in these different approaches to searching.

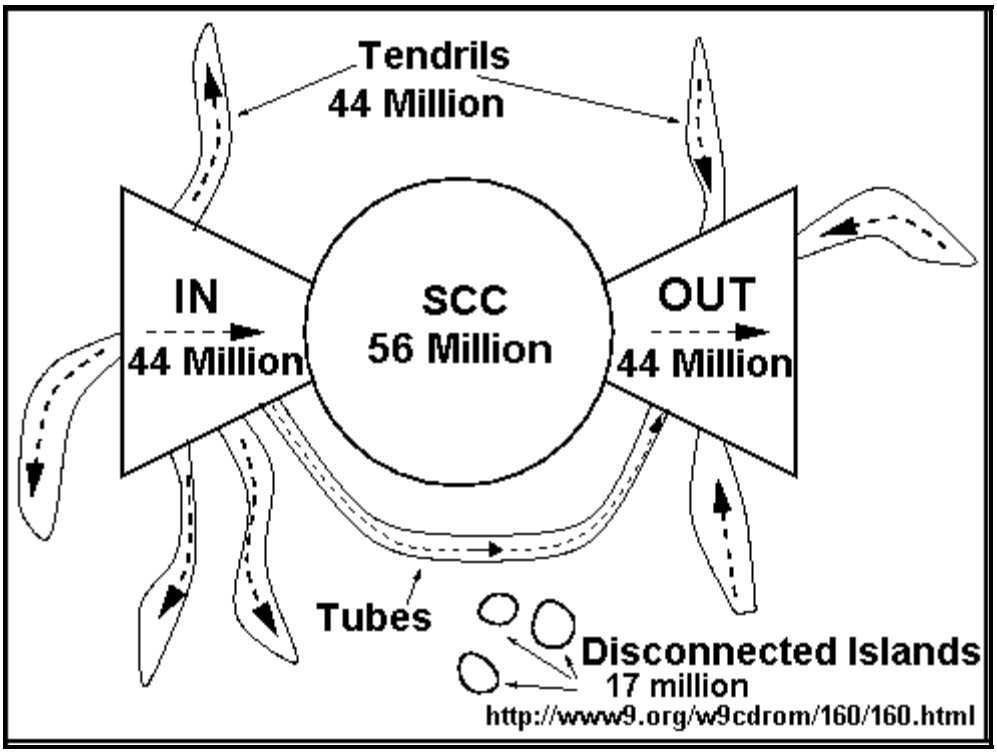
1. You discover a valuable web page called target.html. Most people simply explore the hyperlinks contained within target.html. Those links take you to places suggested by the author of target.html. In short, all you are able to discover are the pages which are located "downstream" of target.html

2. You discover a valuable web page called target.html. In order to help judge the importance, value, popularity of the page, it would be nice to know "How many other web pages contain hyperlinks pointing towards target.html. This shows how many web authors know about the target site, and felt that the site was "good enough" to deserve a hyperlink from their own web site." If a web page looks fairly anonymous, you might be able to infer something about the source of the web page based on who else links toward the web page. Fortunately some search engines (like AltaVista) will allow you to search for all web pages, which contain a hyperlink to a specific URL. This is what is called "searching upstream" of a web page. Here is an example search: the following search would show you what pages link to the White House web site which also have a domain name ending in .jp +link:whitehouse.gov +domain:.jp. Note that some search engines can rank their search results based on the "popularity" of a web paged derived from how many links point toward that web page.

3. You discover two valuable web pages called target.html and other_target.html. If you can find any web pages that link to both of these target pages, then you may discover a great "directory" such as "Joe's list of targets on the Internet" for the subject covered by these target pages.

Here are additional search examples based on Altavista's format:

+link:resource.com	Web pages containing links toward resource.com
+link:resource.com/pageA.html	web pages containing links toward the specific web page
+link:resource1.com +link:resource2.com	Web pages which link towards both resources. This is a good way to discover virtual libraries
+link:newpaper_1.com +link:newspaper_2.com	Web pages which link to these two newspaper (might also link to many other newspapers)
+link:resource.com +domain:.ru	Web pages hosted on .ru machines which contain a hyperlink to resource.com
+link:resource.com +host:gov.ru	Web pages hosted on gov.ru machines which contain a hyperlink to resource.com
+search_term +host:gov.ru	Web pages hosted on gov.ru machines which mention search_term
+host:resource.com	Web pages from Resource.com - can be used to size a web site



Searching upstream is not only a good idea, it is actually **necessary** in order to even reach almost half of all web pages known to Alta Vista

Detailed research paper on this: http://www9.org/w9cdrom/160/160.html

Source: http://navigators.com/search_upstream.html

Annex B: Selected Information Sources

The following Internet resource pages were compiled by the Intelligence Staff of CINCEASTLANT. They provide both a resource of immediate value to analysts as well as some practical examples of how to employ successful Internet-based search strategies in support in a variety of intelligence problems. The date following the titles below represents the last time that the collection was updated.

a. Terrorist Threat Research (Rev 04 Mar 02)

b. Hostile Intelligence Threat Research (15 Feb 02)

c. Criminal Threat Research (15 Feb 02)

d. Medical Threat (Rev 08 May 02)

e. Geo-Political, Military & Country Information Research (Rev 04 Mar 02)

f. Geo-Political & Military Information – Russian Annex (Rev 04 Mar 02)

g. Gazetter, Port, Geodessy and Map Research (Rev 02 May 02)

a. Terrorist Threat Research (Rev 04 Mar 02)

BACKGROUND

Most often, research on terrorist threats will be incorporated into a Force Protection (FP) Threat Summary (THREATSUM) or Briefing. Both of these products should clearly and concisely define the actual and/or potential dangers to a specific allied/coalition force, in a specific geographic area of operations during a specific period of time. ***In all cases, the relevant "raw" research documents should be saved to an appropriate file folder under the country or area of concern.***

GUIDELINES

Confirm or refute the existence of a threat. Traveler warnings and terrorism reports issued by the State Departments or Foreign Ministries of the western governments are probably the best source for general force protection information. These documents provide credible general and specific information about terrorist threats as well as short-term and/or trans-national conditions posing a significant risk to the physical security of Allied/Coalition Force.

- U.S. Department of State Travel Warnings (http://travel.state.gov/travel_warnings. html).

- U.S. Department of State, Crime Control Fact Sheets (http://www.state.gov/g/inl/crm/fs)

- U.S. National Security Council, International Crime Threat Assessment (http://clinton4.nara.gov/WH/EOP/NSC/html/documents/pub45270/pub45270chap3.html

- Canadian Department of Foreign Affairs, Travel Advisories (http://voyage.dfait-maeci.gc.ca/destinations/menue.htm).

- British Foreign and Commonwealth Office travel advice notices (http://193.114. 50.10 /travel/countryadvice.asp).

- U.S. Navy, Office of Naval Intelligence (ONI), Worldwide Threat to Shipping (http://pollux.nss.nima.mil/onit/onit_j_main.html)

- Center for Defense Information (http://www.cdi.org) - This site has weekly articles compiled or produced by academics which include information on world terrorist, weapons of mass destruction, military defense, etc.

Define the historical activities of the specific terrorist and subversive groups/ organizations residing and/or operating in, or transiting through the country or area of interest. The below listed databases provide historical data on a wide variety of well-known groups.

- U.S. Department of State Patterns of Global Terrorism Annual Reports (http://www.state.gov/s/ct/rls/pgtrpt/) provide detailed assessments of foreign countries where significant terrorist acts occurred during the reporting period.

- American Federation of Scientists (FAS) Liberation Movements, Terrorist Organizations, Substance Cartels, and Other Para-State Entities (http://www.fas.org/ irp/ world/para/index.html) is a listing of 370 terrorist/subversive groups (many with hyperlinks to background information). Additionally, Search FAS (http://www.fas. org/) can be used to research the organization's databases.

- U.S. Navy Postgraduate School Terrorist Group Profiles (http://web.nps.navy.mil/ ~library/tgp/tgpndx.htm) is a listing of 370 terrorist/subversive groups (many with hyperlinks to background information).

- International Policy Institute for Counter-Terrorism (http://www.ict.org.il/) is an Israeli-based research database on terrorist organizations and events. Select the "Search Text" icon and enter the terrorist group name to access data.

- Emergency Response & Research Institute, Inc. (ERRI) Counter-Terrorism Archive (http://www.emergency.com/cntrterr.htm) provides information on World-Wide Terrorism Events, Groups, and Terrorist Strategies and Tactics.

- Jane's Information Group (http://www.janes.com/) is a **subscription service** providing access to highly credible data on geo-political, military, intelligence and terrorism issues. However, **free access is authorized to selected items** via Jane's Search (access through the homepage), the Sentinel Risk Pointers (http://www.janes.com/ regional_news/sentinel/risk_pointers.shtml) and International News Briefs (http://www.janes.com/regional_news/international/news_briefs/foreign_report_toc_2001-1.shtml).

- Economist Intelligence Unit (http://www.eiu.com) is a **subscription service** providing access to highly credible data on regional and national geo-political, economic and security issues. However, **free access is authorized to selected items** via the Data Services and ViewsWire web sites contain country specific historical and current political, economic and security information.

- EIU ViewsWire (http://www.viewswire.com/) is a daily country analysis service covering 195 countries and providing an unrivalled and timely database of background information, analysis and forecasts.

- Separatist, Para-military, Military, Intelligence, and Aid Organizations (http://members.home.net/bob.cromwell/security/Index.html#L) is a privately maintained home-page listing a large number of terrorist, subversive and/or "freedom fighter" organizations. Hyperlinks provide access to organization backgrounds.

- Political Terrorism Database (http://polisci.home.mindspring.com/ptd/) is a privately maintained database divided up into geographic areas containing an index to each region's terrorist groups as well as an international terrorism incident database.

- Terrorism Research Center, Calendar of Significant Events (http://www.terrorism. com/calendar/Calendar.html) is a compilation of dates that have importance for terrorism research and analysis.

- National Center for Policy Analysis (NCPA), Terrorism and Nuclear Proliferation archive of articles and press releases concerning the risk of nuclear terrorism (http:// www.ncpa.org/ pi/internat/intdex10.html).

Define current terrorist and subversive activity in the country or area of interest. The below listed databases, metasearch engines and news search engines/sites should be searched employing the search strings indicated below.

- U.S. Department of State, Overseas Security Advisory Council (OSAC) Daily Global News (http://www.ds-osac.org/globalnews/default.cfm) keyword search provides timely information on foreign events related to security.

- Vivisimo (http://www.vivisimo.com/) a high quality metasearch engine.

- Ixquick (http://www.ixquick.com/) a high quality metasearch engine supplementing Vivisimo.

- NewsTrawler (http://www.newstrawler.com/nt/nt_home.html) is a metasearch engine for news archives and articles from worldwide sources. Search categories are By Country, Across Countries, Category and Across Categories.

- The Ultimate Collection of News Links (http://pppp.net/links/news/) is a reference source of media hyperlinks by region and country. Conduct searches of the appropriate news media source(s) in the country or area of interest.

- News Index (http://www.newsindex.com) is a search engine for current news stories from worldwide sources.

- Pandia Newsfinder (http://www.pandia.com/news/index.html) is a search engine for current news and links to news sources.

- AlertNet (www.alertnet.org) is a Reuters-sponsored service providing global news, communications and logistics services to the international disaster relief community. The public pages, accessible to anyone, carry a live news feed and articles describing how relief agencies are responding to the latest humanitarian crises.

- BBC World Service (http://www.bbc.co.uk/worldservice/).

Use standard "search strings" employing simple Search Engine Math or Boolean Logic commands such as those listed below.

- *terrorist/subversive group name*
- *country name* **+terrorism**
- *country name* **+extremist***
- *country name* **+subversive**
- *country name* **+underground**
- *country name* **+bomb***
- *country name* **+explosion**
- *country name* **+assassin***
- *country name* **+arson**
- *country name* **+kidnap***
- *country name* **+demonstration**

b. Hostile Intelligence Threat Research (15 Feb 02)

BACKGROUND

Counterintelligence is a critical element of the Force Protection Threat Summary; however, the availability of credible open source databases and profiles on civilian and military intelligence services is extremely limited. To clearly define the actual and/or potential threat to allied/coalition forces, the analyst probably will have to rely heavily on news articles obtained from multi-national, regional and/or local media sources. ***In all cases, the relevant "raw" research documents should be saved to an appropriate file folder under the country or area of concern.***

GUIDELINES.

Identify the hostile intelligence service(s) residing and/or operating in the country or area of interest.

- American Federation of Scientists (FAS), World Intelligence and Security Agencies page (http://www.fas.org/irp/world/index.html) provides hyperlinks to profiles on intelligence agencies of selected countries.

- Jane's Information Group (http://www.janes.com/) is a **subscription service** providing access to highly credible data on geo-political, military, intelligence and terrorism issues. However, **free access is authorized to selected items** via Jane's Search (access through the homepage), the Sentinel Risk Pointers (http://www.janes.com/ regional_news/sentinel/risk_pointers.shtml) and International News Briefs (http://www.janes.com/regional_news/international/news_briefs/foreign_report_toc_2001-1.shtml).

- Economist Intelligence Unit (http://www.eiu.com) is a **subscription service** providing access to highly credible data on regional and national geo-political, economic and security issues. However, **free access is authorized to selected items** via the Data Services and ViewsWire icons.

Define historical and current hostile intelligence activities that may be directed against allied/coalition forces. The below listed databases, metasearch engines and news search engines/sites should be searched employing the search strings indicated in paragraph B.2.3.

- U.S. Department of State, Overseas Security Advisory Council (OSAC) Daily Global News (http://www.ds-osac.org/globalnews/default.cfm) keyword search provides timely information on foreign events related to security.

- Vivisimo (http://www.vivisimo.com/) a high quality metasearch engine.

- Ixquick (http://www.ixquick.com/) a high quality metasearch engine supplementing Vivisimo.

- NewsTrawler (http://www.newstrawler.com/nt/nt_home.html) is a metasearch engine for news archives and articles from worldwide sources. Search categories are By Country, Across Countries, Category and Across Categories.

- The Ultimate Collection of News Links (http://pppp.net/links/news/) is a reference source of media hyperlinks by region and country. Conduct searches of the appropriate news media source(s) in the country or area of interest.

- News Index (http://www.newsindex.com) is a search engine for current news stories from worldwide sources.

- Pandia Newsfinder (http://www.pandia.com/news/index.html) is a search engine for current news and links to news sources.

- AlertNet (www.alertnet.org) is a Reuters-sponsored service providing global news, communications and logistics services to the international disaster relief community. The public pages, accessible to anyone, carry a live news feed and articles describing how relief agencies are responding to the latest humanitarian crises.

- BBC World Service (http://www.bbc.co.uk/worldservice/).

- Economist Intelligence Unit (EIU, http://www.eiu.com) electronic data requires a subscription or fee for individual articles. However, the Data Services and ViewsWire web sites contain country specific historical and current political, economic and security information.
-
 - EIU ViewsWire (http://www.viewswire.com/) is a daily country analysis service covering 195 countries and providing an unrivalled and timely database of background information, analysis and forecasts.

Use standard "search strings" employing simple Search Engine Math or Boolean Logic commands such as those listed below.

- *name of the national intelligence service(s)*
- *country name* **+intelligence**
- *country name* **+counterintelligence**
- *country name* **+espionage**
- *country name* **+security**
- *country name* **+spy**
- *country name* **+surveillance**
- *country name* **+clandestine**
- *country name* **+secret**
- *country name* **+secret** +**police**
- *country name* **+underground**
- *country name* **+covert**

c. Criminal Threat Research (15 Feb 02)

BACKGROUND

Most often, research on criminal threats and the availability of drugs will be incorporated into a Force Protection (FP) Threat Summary (THREATSUM) or Briefing. Both of these products should clearly and concisely define the actual and/or potential dangers to a specific allied/coalition force, in a specific geographic area of operations during a specific period of time. ***In all cases, the relevant "raw" research documents should be saved to an appropriate file folder under the country or area of concern.***

GUIDELINES.

Identify the criminal threats and define the availability of drugs. Traveler warnings and annual crime/drug reports issued by the State Departments or Foreign Ministries of the western governments are probably the best source of general information about the significant risks to Allied/Coalition Forces.

- U.S. Department of State Travel Warnings (http://travel.state.gov/travel_ warnings. html).
- U.S. Department of State, Crime Control Fact Sheets (http://www.state.gov/ g/inl/crm/fs).
- U.S. National Security Council, International Crime Threat Assessment (http://clinton4.nara.gov/WH/EOP/NSC/html/documents/pub45270/pub45270 chap3.html).
- Canadian Department of Foreign Affairs, Travel Advisories (http://voyage. dfait-maeci.gc.ca/destinations/menue.htm).
- British Foreign and Commonwealth Office travel advice notices (http:// 193.114. 50.10 /travel/countryadvice.asp).
- U.S. Department of State, International Narcotics Control Strategy Annual Report (http://www.state.gov/g/inl/rls/nrcrpt/).
- United Nations, Global Illicit Drug Trends (http://www.odccp.org/global _illicit_drug_trends.html)

Define current criminal activity in the country or area of interest. The below listed databases, metasearch engines and news search engines/sites should be searched employing the search strings indicated in paragraph C.2.3.

- Vivisimo (http://www.vivisimo.com/) a high quality metasearch engine.

- Ixquick (http://www.ixquick.com/) a high quality metasearch engine supplementing Vivisimo.

- NewsTrawler (http://www.newstrawler.com/nt/nt_home.html) is a metasearch engine for news archives and articles from worldwide sources. Search categories are By Country, Across Countries, Category and Across Categories.

- The Ultimate Collection of News Links (http://pppp.net/links/news/) is a reference source of media hyperlinks by region and country. Conduct searches of the appropriate news media source(s) in the country or area of interest.

- News Index (http://www.newsindex.com) is a search engine for current news stories from worldwide sources.

- Pandia Newsfinder (http://www.pandia.com/news/index.html) is a search engine for current news and links to news sources.

Use standard "search strings" employing simple Search Engine Math or Boolean Logic commands such as those listed below.

- *country name* **+crime**
- *country name* **+robbery**
- *country name* **+mafia**
- *country name* **+assault**
- *country name* **+trafficking**
- *country name* **+narcotics**
- *country name* **+ drugs**

d. Medical Threat *(Rev 08 May 02)*

BACKGROUND.

Most often, research on medical issues will be incorporated into a Force Protection (FP) Threat Summary (THREATSUM) or Briefing. Both of these products should clearly and concisely define the actual and/or potential dangers to a specific allied/coalition force, in a specific geographic area of operations during a specific period of time. In all cases, the relevant "raw" research documents should be saved to an appropriate file folder under the country or area of concern.

GUIDELINES.

1. Identify the types of disease and other significant environmental risks present in the area of interest. Traveler warnings issued by the State Departments or Foreign Ministries of the western governments are probably the best source of general information about the actual and/or potential medical dangers to Allied/Coalition Forces.

- U.S. Department of State Travel Warnings (http://travel.state.gov/travel_ warnings. html).

- Canadian Department of Foreign Affairs, Travel Advisories (http://voyage. dfait-maeci.gc.ca/destinations/menue.htm).

- British Foreign and Commonwealth Office travel advice notices (http:// 193.114. 50.10 /travel/countryadvice.asp).

2. Determine if there has been a recent (with the last year) outbreak of disease or a rise in the incidence of other significant environmental risks in the area of interest. The following databases, metasearch engines and news search engines/sites should be consulted.

- World Health Organization (http://www.who.int/home-page/)

- Center for Disease Control (http://www.cdc.gov/travel/reference.htm)

- International Society of Travel Medicine (http://www.istm.org/) is a global organization dedicated to healthy and safe travel medicine and international care.

- U.S. Department of State HIV/AIDS and Emerging Infectious Diseases (http://www.state.gov/g/oes/hlth/).

3. If no significant data is found or more information is required, conduct searches using news search engines.

e. Geo-Political, Military & Country Information Research (Rev 04 Mar 02)

POLITICAL LEADERS

– U.S Department of State, Chiefs of State and Cabinet Members of Foreign Governments (http://www.odci.gov/cia/publications/chiefs/index.html) provides a listing of government officers.

MILITARY INFORMATION

- American Federation of Scientists (FAS), Military Analysis Network (http://www.fas.org/man/index.html) provides links to military order of battle information. Additionally, Search FAS (http://www.fas.org/) can be used to research the organization's databases.

- Jane's Information Group (http://www.janes.com/) is a **subscription service** providing access to highly credible data on geo-political, military, intelligence and terrorism issues. However, **free access is authorized to selected items** via Jane's Search (access through the homepage), the Sentinel Risk Pointers (http://www.janes.com/regional_news/sentinel/risk_pointers.shtml) and International News Briefs (http://www.janes.com/regional_news/international/news_briefs/foreign_report_toc_2001-1.shtml).

- Center for Defense Information (http://www.cdi.org) - This site has weekly articles compiled or produced by academics which include information on world terrorist, weapons of mass destruction, military defense, etc.

COUNTRY BACKGROUND INFORMATION

- U.S Department of State, Background Notes (http://www.state.gov/countries/, http://www.state.gov/r/pa/bgn/) provide historical geo-political, economic and social information on most nations of the world.

- Library Of Congress, Country Studies Country Studies On-Line (http://lcweb2.loc.gov/frd/cs/) presents a description and analysis of the historical setting and the social, economic, political, and national security systems and institutions of countries throughout the world. Information is not copyrighted and thus is available for free and unrestricted use by researchers. As a courtesy, however, appropriate credit should be given to the series.

- U.S. Central Intelligence Agency (CIA), World Factbook (http://www.odci.gov/cia/publications/factbook/index.html) provides access to historical social,

economic, political, and national security information on countries throughout the world.

- American Federation of Scientists (FAS), Country Studies (http://www.fas.org/news/index.html) provides background information on national security, military, intelligence and medical information. Additionally, Search FAS (http://www.fas.org/) can be used to research the organization's databases.

- Lonely Planet Travel Guide (http://www.lonelyplanet.com/destinations/) provides historical cultural and social information on the countries of the world.

- Economist Intelligence Unit (http://www.eiu.com) is a **subscription service** providing access to highly credible data on regional and national geo-political, economic and security issues. However, **free access is authorized to selected items** via the Data Services and ViewsWire web sites which contain country specific historical and current political, economic and security information.

 - EIU ViewsWire (http://www.viewswire.com/) is a daily country analysis service covering 195 countries and providing an unrivalled and timely database of background information, analysis and forecasts.

f. Geo-Political & Military Information – Russian Annex (Rev 04 Mar 02)

RUSSIAN MILITARY

http://www.webcom.com/~amraam/shipind.html - A site containing information on Russian ships and submarines currently active and in which fleet they belong. This site can be used as an additional source, or to supplement classified information.

RUSSIAN NEWS

http://en.rian.ru/rian/index.cfm - Russia Information Agency - A daily news site like BBC. Information appears on this site for two days before it is put into an archive and must be paid for.

http://www.gazeta.ru/english - Gazeta. This site contains Russian information that is updated on a daily basis.

http://www.interfax.com/com?item=Rus - Interfax. This site contains economic news from Russia.

http://www.itar-tass.com/newsdir.htm - ITAR-TASS. This site only gives headlines. The details of articles must be purchased. Small photos are also available.

http://www.russianobserver.com - Articles on this site are updated on an irregular basis. Checking this site weekly is sufficient.

http://www.therussianissues.com - Articles on this site are updated on an irregular basis. Checking this site weekly is sufficient.

http://www.smi.ru - Russian version of The Russian Issues. Can be translated using a web translator such as Babel fish.

http://www.themoscowtimes.com - In English. This paper is updated on a daily basis.

http://www.cdi.org/russia - This site contains the Russia Weekly, which is a weekly report compiled from articles from various sources. The site is updated on Fridays, and should be checked weekly. It also contains a link to Moscow Times.

http://www.adresa.ru - Another Russian site. Must be translated.

http://www.vesti.ru - Russian paper updated on a daily basis. Must be translated.

g. Gazetter, Port, Geodessy and Map Research *(Rev 02 May 02)*

GAZETTEER (Database of geographic feature names)

- U.S. National Imagery and Mapping Agency, GEOnet Names Server (GNS) Gazetteer (http://gnpswww.nima.mil/geonames/GNS/index.jsp) provides access to worldwide (excluding the U.S. and Antarctica) geographic feature names. For names in the U.S. and Antarctica go to the US Geological Survey (USGS, http://geonames.usgs.gov/).

- Global Gazetteer (http://www.calle.com/world/) is a directory of 2880532 of the world's cities and towns, sorted by country and linked to a map for each town. Presentation Copyright 1998-2000 by Falling Rain Genomics, Inc.

PORT INFORMATION

- U.S. National Imagery and Mapping Agency, World Port Index Pub 150 (http://pollux.nss.nima.mil/pubs/pubs_j_wpi_sections.html). Documents are in PDF format and require Adobe Acrobat Reader.

- World Port Directory (www.maxpages.com/port) is a commercial internet webpage providing information on selected ports of the world and waterways frequented by cruise ships.

MAPPING AND GEODESY PRODUCTS

- U.S. National Imagery and Mapping Agency Geospatial Engine (http://geoengine.nima.mil) provides access to imagery of the Earth, maps and other geospatial information.

- U.S. National Imagery and Mapping Agency, Aeronautical Information Homepage (http://164.214.2.62/products/digitalaero/index.html) provides access to global aeronautical geospatial information and services to include the Digital Aeronautical Flight Information File (DAFIF®), Flight Information Publications, FLIP Planning Documents and Enroute Supplements, and Prototype Terminal Instrument Procedures and Airport Diagrams.
 - Documents are in PDF format and require Adobe Acrobat Reader.
 - Also accessible via the NIMA Map and Geospatial Data web page (http://164.214.2.59/geospatial/geospatial.html).

- Earth-Info Navigation Page (http://www.earth-info.org/JavaGlobeStart.html), provides access to a world of imagery, maps, and other information. Hyperlinks are available to the CIA World Factbook (http://www.odci.gov/

cia/publications/factbook/index.html), ImageLinks, ImageNet, DOI-10 Imagery DTED Select DOI-10 Imagery, DTED® 0 Terrain Data, VMap 0 Vector Map, VMap 1 Vector Map, ONC Raster Map, TPC Raster Map and National Geographic geodesy products.
 - Also accessible via the NIMA Map and Geospatial Data web page (http://164.214.2.59/geospatial/geospatial.html).

- U.S. Central Intelligence Agency World Factbook (http://www.odci.gov/cia/publications/factbook/index.html) provides access to regional and country geopolitical maps.

- Lonely Planet Travel Guide (http://www.lonelyplanet.com/destinations/) provides access to country and city tourist maps.

NAVAL POSTGRADUATE SCHOOL
Monterey, California



THESIS

OPEN-SOURCE INTELLIGENCE IN THE CZECH MILITARY: KNOWLEDGE SYSTEM AND PROCESS DESIGN

by

Roman Krejci

June 2002

Thesis Advisor: Mark E. Nissen
Second Reader: Kenneth R. Dombroski

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2002	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Open-Source Intelligence in the Czech Military: Knowledge System and Process Design			**5. FUNDING NUMBERS**
6. AUTHOR(S) Roman Krejci			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT

Owing to the recent transitions in the Czech Republic, the Czech military must satisfy a large set of new requirements. One way the military intelligence can become more effective and can conserve resources is by increasing the efficiency of open-source intelligence (OSINT), which plays an important part in intelligence gathering in the age of information. When using OSINT effectively, the military intelligence can elevate its responsiveness to different types of crises and can also properly allocate its limited resources into areas, in which covert collection is unavoidable.

This thesis combines modern knowledge-management theory with current issues in military intelligence, creating a base for designing a future OSINT system in the Czech military. First, the thesis introduces recent US research in knowledge management and examines the current intelligence issues. Then the thesis examines the Czech military intelligence environment in the framework of the national security and defense policy and also analyzes the actual use of OSINT in the Military Intelligence Service, following the four stages of the knowledge system and process design. Finally, the thesis outlines the main aspects of the future OSINT knowledge-management system and recommends further research and development.

14. SUBJECT TERMS Knowledge Management, Intelligence, Open-Source Intelligence, Czech Military			**15. NUMBER OF PAGES** 133
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

OPEN-SOURCE INTELLIGENCE IN THE CZECH MILITARY: KNOWLEDGE SYSTEM AND PROCESS DESIGN

Roman Krejci
Lieutenant Colonel, Army of the Czech Republic
ing., Military College Vyskov, CZ, 1985

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 2002

Author: Roman Krejci

Approved by: Dr. Mark E. Nissen
Thesis Advisor

Kenneth R. Dombroski
Second Reader

Douglas A. Brook, Ph.D.
Dean, Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Owing to the recent transitions in the Czech Republic, the Czech military must satisfy a large set of new requirements. One way the military intelligence can become more effective and can conserve resources is by increasing the efficiency of open-source intelligence (OSINT), which plays an important part in intelligence gathering in the age of information. When using OSINT effectively, the military intelligence can elevate its responsiveness to different types of crises and can also properly allocate its limited resources into areas, in which covert collection is unavoidable.

This thesis combines modern knowledge-management theory with current issues in military intelligence, creating a base for designing a future OSINT system in the Czech military. First, the thesis introduces recent US research in knowledge management and examines the current intelligence issues. Then the thesis examines the Czech military intelligence environment in the framework of the national security and defense policy and also analyzes the actual use of OSINT in the Military Intelligence Service, following the four stages of the knowledge system and process design. Finally, the thesis outlines the main aspects of the future OSINT knowledge-management system and recommends further research and development.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. THESIS SUBJECT, OBJECTIVES, AND RESEARCH APPROACH 1
A. BACKGROUND 1
B. OBJECTIVES 2
C. RESEARCH QUESTION 3
D. SCOPE, LIMITATIONS, AND ASSUMPTIONS 3
E. OVERVIEW OF THE RESEARCH APPROACH 4

II. LITERATURE REVIEW AND THEORETICAL FRAMEWORK 5
A. KNOWLEDGE MANAGEMENT 5
1. Data, Information, and Knowledge 6
2. Knowledge Management and Knowledge Flow 9
3. Knowledge Management Life Cycle 11
4. Knowledge System and Process Design 13
B. INTELLIGENCE AND MILITARY INTELLIGENCE 17
1. Intelligence Functions and Intelligence Disciplines 17
2. Intelligence Process and Intelligence Cycle 19
3. Common Problems and Challenges in Intelligence 23
C. OPEN-SOURCE INTELLIGENCE (OSINT) 27
1. Definitions and Categories 27
2. Problems and Challenges in Open-Source Intelligence 31

III. CZECH MILITARY, INTELLIGENCE, AND OSINT 39
A. CZECH SECURITY ENVIRONMENT AND THE MILITARY 39
1. New Security Environment 39
2. Current Threats and Risks to Czech National Security 41
3. Czech Military 43
B. CZECH INTELLIGENCE AND COUNTER-INTELLIGENCE SERVICES 51
1. Services, Tasks, Cooperation, and Oversight 52
2. Current Military Intelligence Requirements 55
C. OSINT IN THE CZECH MILITARY INTELLIGENCE SERVICE 61
1. Process Analysis 62
2. Knowledge Analysis 64
3. Context Analysis 67
4. Systems Analysis 68

IV. ADAPTING KNOWLEDGE MANAGEMENT THEORY TO THE CZECH MILITARY INTELLIGENCE 79
A. MAJOR STEPS TO BUILDING OSINT KNOWLEDGE-MANAGEMENT SYSTEM 79
B. OBJECTIVES AND LIMITATIONS TO BUILDING OSINT KNOWLEDGE-MANAGEMENT SYSTEM 83
1. OSINT Knowledge Management Process 83
2. Organizational Design 87
3. Challenges Specific to the Czech Military Intelligence 92

C. OSINT KNOWLEDGE MANAGEMENT PROCESS AND SYSTEM DESIGN 93
1. Facilitating Knowledge Flow 94
2. Organization of the OSINT Knowledge-Management System 99
V. CONCLUSIONS AND RECOMMENDATIONS 103
A. SIGNIFICANCE OF SYSTEM APPROACH 103
B. ORGANIZATIONAL ISSUES 105
C. RECOMMENDATIONS FOR FURTHER RESEARCH AND DEVELOPMENT 106
LIST OF REFERENCES AND WORKS CITED 109
INITIAL DISTRIBUTION LIST 115

LIST OF FIGURES AND GRAPHS

Figure 1. Knowledge Hierarchy 8
Figure 2. Knowledge Management Life Cycle 11
Figure 3. Amended Model of the Intelligence Cycle 20
Figure 4. Organizational Structure of the ACR 47
Figure 5. Organizational Structure of the ACR by 2007 50
Figure 6. Subordination of the Military Intelligence Services 52
Figure 7. Four Strategies for Knowledge Management and the VZS 69
Figure 8. Controlling and Collaboration in the VZS 72
Figure 9. Collection Coordination and Information Requirements Management in the VZS 73
Figure 10. Military Intelligence and Knowledge Interaction Modes 74
Figure 11. Loose Organization of OSINT Units 89
Figure 12. OSINT Knowledge Flow and IT infrastructure 98
Figure 13. Four Strategies for Knowledge Management and the Future VZS 99
Figure 14. Virtual OSINT Organization 102

Graph 1. Frequency of the Use of Domestic Open Sources 75
Graph 2. Frequency of the Use of Foreign Open Sources 76

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Characteristics of the Extant Organizational Design and IT in the VZS 70
Table 2. Characteristics of the Future Organizational Design and IT in the VZS 100

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS

ACE	Allied Command in Europe
ACR	Army of the Czech Republic
AJP	Allied Joint Publication
ARCTSC	Analysis of Required Capabilities, Target Structure and Composition
BBC	British Broadcasting Corporation
BIS	Bezpečnostní informační služba (Security Information Service)
C4I	Command, Control, Communication, Computers, and Intelligence
CBW	Chemical and Biological Weapons
CCIRM	Collection Coordination and Information Requirements Management
CD	Compact Disc
CD-ROM	Compact Disc—Read Only Medium
CEDSP	Common European Security and Defense Policy
CIA	Central Intelligence Agency
CIMIC	Civil-Military Cooperation
CIO	Chief Information Officer
CKO	Chief Knowledge Officer
CNN	Cable News Network
COMINT	Communication Intelligence
COTS	Commercial Off-the-Shelf
CSFs	Critical Success Factors
DBMS	Database Management System
DBK	Dominant Battlespace Knowledge
DVD	Digital Video Disc
DW/DM	Data Warehouse/Data Mining
DoD	Department of Defense
ELINT	Electronic Intelligence
EU	European Union
ES	Expert Systems
FAS	Federation of American Scientists
FBIS	Foreign Broadcast Service
HUMINT	Human Intelligence
ICBM	Inter-Continental Ballistic Missiles
IMINT	Imagery Intelligence
INFOSEC	Information Security
INTs	Intelligence Disciplines
IT	Information Technology
KBS	Knowledge-Based System
KMLC	Knowledge Management Life Cycle
MASINT	Measurement and Signature Intelligence
NATO	North Atlantic Treaty Organization
NIPRNET	National Internet Protocol Routing Network
NMS	National Military Strategy

NOSINTH	NATO Open-Source Intelligence Handbook
NSS	National Security Strategy
OSINT	Open-Source Intelligence
OSINTH	Open-Source Intelligence Handbook
OSIS	Open-Source Information Network
PCR	Police of the Czech Republic
PEO	Peace Enforcement Operations
PfP	Partnership for Peace
PKO	Peace Keeping Operations
R&D	Research and Development
SIGINT	Signal Intelligence
SSL	Secure Sockets Layers
StB	Státní bezpečnost (State Security)
UN	United Nations
ÚZSI	Úřad pro zahraniční styky a informace (Bureau for Foreign Contacts and Information)
V-OSINT	Validated Open-Source Intelligence
VOZ	Vojenské obranné zpravodajství (Military Defensive Intelligence)
VPN	Virtual Private Network
VZ	Vojenské zpravodajství (Military Intelligence)
VZS	Vojenská zpravodajská služba (Military Intelligence Service)
WMD	Weapons of Mass Destruction
ZZS	Zákon o zpravodajských službách (Intelligence Services Act)

ACKNOWLEDGMENTS

The work I accomplished could be hardly possible without the help and support of many people.

I would like to thank my supervisor and my colleagues for all the support and goodwill that allowed me to study at the Naval Postgraduate School. Also, I want to acknowledge my professors and lecturers, who led me through the studies—particularly Prof. John Arguilla for his excellent insight into the military matters and astounding clear-headedness of an exceptional thinker. Many thanks to my thesis advisor, Dr. Mark Nissen, and to my second reader, Kenneth Dombroski, for their candid approach and unstrained facilitation of my research and thesis work. Furthermore, I want to thank my thesis editor, Ronald Russell, for his excellent, highly professional editorial work, and also for his friendship. Finally, my greatest appreciation goes to my wife Věra, my daughter Jana, and my son Víťa for their patience and support while I completed this work.

THIS PAGE INTENTIONALLY LEFT BLANK

I. THESIS SUBJECT, OBJECTIVES, AND RESEARCH APPROACH

Chapter one discusses the purpose and objectives of this thesis. It presents brief background information and the research questions. The chapter also provides an overview of the research approach and describes its scope, limits, and assumptions.

A. BACKGROUND

The Czech military intelligence needs to evolve into a different type of service—for several reasons. Recent political, economical, and social transitions have imposed different security threats on the Czech Republic. Moreover, accession to NATO has brought a large set of requirements that military intelligence must meet. In addition, the information revolution presents permanent challenges for intelligence collection and processing.

Indeed, much has already changed since the peaceful revolution in 1989. However, many of the military intelligence procedures and assets remain frozen in an old-fashioned mindset. The economical and political disposition of the Czech government during the mid-1990's left the top military management with many unanswered questions. Furthermore, frequent ad hoc adjustments in both organizational and procedural arrangements have not significantly helped the military intelligence to move ahead.

It is obvious that the Czech Republic does not have, and will unlikely ever have, the collection and processing capabilities of the major powers, such as the USA, Canada, and the UK. The Armed Forces of the Czech Republic, limited by budget constraints and by the sociopolitical situation inside the country, cannot simply make a huge leap toward state-of-the-art military technologies. However, if the top management of military intelligence really wants to improve the service, a systematic and scientific approach is necessary in order to achieve positive results.

One way to increase intelligence effectiveness and conserve resources is to employ *open-source intelligence* (OSINT) efficiently. Military intelligence should fully embrace all the advantages of OSINT, which plays an important part in intelligence gathering in the age of information. When using OSINT effectively, the military intelligence can elevate its responsiveness to different types of current crises and can also allow the proper allocation of its limited resources into other areas, in which covert collection is unavoidable.

Although the Czech military intelligence currently uses open sources for gaining different kinds of information, a systematic approach to this domain has been missing and the use of OSINT is far from an ideal solution. However, by building upon the framework of knowledge management theory, a basic design of modern OSINT in the Czech military intelligence can be created. Such an arrangement can then be considered as a base for further research and development in this area.

B. OBJECTIVES

On one side, knowledge management theory and its implications represent a new arena for the Czech military, an arena that has not been explored yet. On the other side, using open sources for intelligence purposes was significant even in the pre-revolution information gathering. But OSINT was practically abandoned in the early 1990's and has not been systematically modernized since then.

This thesis seeks to meet the following objectives:

- To introduce recent US research in knowledge management to the Czech military environment.
- To indicate contemporary problems in intelligence and to examine current knowledge about OSINT.
- To inquire the military intelligence environment in the framework of the Czech security and defense policy, and to analyze actual use of OSINT in the intelligence.
- To create a theoretical base for future design of OSINT systems and processes in the Czech military intelligence.

- To make a set of recommendations for further research and development.

C. RESEARCH QUESTION

This research is focused on answering a primary question "How can the Czech military intelligence design its open-source intelligence?" To help answer the question, these subsequent secondary questions will be addressed:

- What is knowledge, and how is it used in military intelligence processes?
- What is open-source intelligence (OSINT), and how does it contribute to military intelligence?
- What is the current status of OSINT in the Czech military intelligence?
- How can the basic steps of knowledge system and process design be used to model the improved OSINT in the Czech military intelligence?
- What recommendations can be made for the Czech military intelligence management?

D. SCOPE, LIMITATIONS, AND ASSUMPTIONS

The scope of this thesis includes an overview of knowledge management theory. Also, the thesis provides a current view of intelligence in general, and further concentrates on the currently most auspicious discipline, open-source intelligence (OSINT). The author builds on the extant security and defense policy of the Czech Republic and examines the present approach to using OSINT in the Czech military intelligence. Most of the attention is paid to the strategic level, represented by the Military Intelligence Service (VZS). However, other levels are included whenever possible in order to provide for wider context in OSINT knowledge management process and system design.

The author does not look for particular information technology (IT) solutions in terms of hardware and software procurement. Moreover, purely IT oriented solution are always interim and provide only temporary competitive advantage. Neither does the author want to create a complete organizational model. For such a goal, specialized teams

and whole sets of introductory steps would be needed. So, the thesis stresses valid principles, taken from both the knowledge management theory and the current literature about intelligence, and establishes a base, upon which the further development of OSINT in the Czech military intelligence can be made.

Also, the thesis does not strive to serve as an account of available open sources. A complete account is not possible owing to the volume and dynamics of OSINT. Even for one single area of interest, an extract of available open sources will be intensely discriminative. So the references to open sources used in this thesis will serve only for explanatory purposes and as examples.

E. OVERVIEW OF THE RESEARCH APPROACH

The research techniques used for this thesis include a review of topical literature related both to knowledge management and intelligence. Also, a review of current Czech military doctrines and policies is performed. Subsequently, a deductive and inductive approach is applied to conduct an analysis of the author's own observations related to OSINT in the Czech military intelligence. This analysis is also accompanied by the results of semi-structured interviews with Czech intelligence staff members. Finally, a knowledge management framework is used to create an introductory design of the OSINT system and processes in the Czech military intelligence.

II. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

This chapter outlines the basic aspects of knowledge management. It also looks at intelligence in general and open-source intelligence (OSINT) in particular in order to create sufficient theoretical background for further use.

The first part of the chapter briefly introduces the current understanding of knowledge, knowledge management, and the knowledge process and system design. The next section examines the body of knowledge about intelligence in general. The last part concentrates on open-source intelligence in more details.

A. KNOWLEDGE MANAGEMENT

Knowledge is power. This expression has not changed much over time. But the importance of such power has changed, owing to the evolution of technological tools that can be used to manage knowledge. The recent widespread advances in computer and communication technologies are usually labeled as the *information revolution*. While the new technology has reached every possible corner of the business world, the military with its highly hierarchical structure struggles to achieve interconnectivity and information superiority in the future battlespace.

Owens (2000) and others argue that the information revolution and advances in computer technology have brought unfailing possibilities for future combat. Such optimistic exponents believe that the advances in computing and communication are truly revolutionary and will change the very nature of the military. According to them, widespread knowledge about potential and existing adversaries—enabled by computer networks, advanced overhead surveillance, and real-time communication—will allow armies to wage better wars. In such an environment of *Dominant Battlespace Knowledge* (DBK), the military will be smaller yet stronger and more mobile, able to react on a short notice. Through the use of advanced information technology, the friendly forces should be better protected and employed more wisely while the enemy forces will be shattered—mostly thanks to the ability to find and track all important enemy assets promptly.

Opposing Owens' views, O'Hanlon (2000) and others see certain disparities in the military assets evolution and argue that while there has been very significant progress in computing and communication systems, there are many other areas where the limits are still severe and evolution slow. Constraints will still remain significant in infantry and urban warfare; optical and radar penetrability of forests and buildings will probably not be improved radically; acoustic and other types of sensors are unlikely to increase their reach dramatically; and detection of chemical and biological materials will likely remain severely limited unless the agents are released out of their carriers.

Many lessons can be learned from the recent developments in the intelligence community. Indeed, the Czech military intelligence should not be built on purely technical premises. On the other hand, proper application and systematic use of technological tools will help to manage knowledge effectively.

1. Data, Information, and Knowledge

In order to understand knowledge and knowledge management principles better, one must clearly distinguish *knowledge* from *information* and *data*. People commonly use "data" and "information" as synonyms while "knowledge" is more clearly viewed as the data or information that people retain in their minds. As the three terms are sometimes used interchangeably, they must be defined at the onset.

Data: Data are most frequently perceived as being related to computer and communication technology. Few authors even bother to define the term, assuming that its meaning is so obvious that it does not require classification. Many misunderstandings can arise from failing to consider the meaning of such a basic concept.

On the academic basis, Clarke (2001/1) provides one useful and simple definition: "Data are any symbol, sign or measure in a form that can be directly captured by a person or a machine." On the military side, the US Department of Defense (DoD), for example, uses this definition of data: [Data represent facts, concepts, or instructions, such as characters or analog quantities, to which meaning is or might be assigned. Data exist in

a formalized manner, suitable for communication, interpretation, or processing by humans or by automatic means.] (JP-1.02. 1994)

So data are understood as a set of discrete facts and events, such as text, numbers, signs, and so on. By itself, data have no meaning until placed in an appropriate context and transferred into information.

Information: The term "information" also requires a proper definition. Dictionaries are usually too vague and different researchers often bring inconsistent definitions. Clarke (2001/1), for example, provides for a definition by encapsulating these elements: "Information is data that has value. Informational value depends upon context. Until it is placed in an appropriate context, data are not information, and once it ceases to be in that context it ceases to be information." A definition invoked in the NATO military intelligence only states that "Information is unprocessed data of every description that may be used in the production of intelligence." (AJP-2.0. 2001) One can see that these definitions do not agree—while the former accentuates information value that is built upon data, the latter merely states information serves as base for an intelligence product.

Information should be understood as a message that possesses meaning; that is what distinguishes it from data, which have no significance on its own. The meaning need not to be the same in the minds of both the sender and receiver. Actually, it is the receiver's cognition what makes the data become information (Davenport and Prusak 1998).

Knowledge: The term "knowledge" is often used to refer to "a body of facts and principles accumulated by mankind in the course of time" (Clarke 2001/2). This is just one of many definitions, but it precisely expresses the necessity of human ability to build knowledge and also the dependence of knowledge on time. This definition also shows that knowledge is based upon previously gained information.

As to the forms in which knowledge can exist, theory distinguishes two main categories—*explicit* knowledge and *inferred* knowledge.

Explicit knowledge is formal, structured, and readily accessible. It can be found in books, manuals, instructions, on the Web, in groupware, and databases (Nonaka 1994,

Nissen 2001). Explicit knowledge is easier to manage and is better supported by existing IT tools. Optimally, an organization should aspire to capture and to use as much knowledge as possible in this form.

Tacit, or *inferred*, *knowledge* is informal, unstructured, and can be accessed only via eduction and observation of behavior (Liebowitz 1999). Tacit knowledge refers to expertise contained within the minds of people (Nonaka 1994, Nissen 2001). It is hard, if not impossible, to transfer it to an explicit form; inferred knowledge is difficult to manage.

In relation to these two categories, one should see that transfer of knowledge can occur either through *structured media* (such as documents and books) in the case of explicit knowledge, or by *interpersonal contacts* (such as conversation, training, apprenticeship, and so on) in the latter instance.

Nissen et al. (2000) summarized work of scholars concerning the distinction between data, information, and knowledge according to their *abundance* and *actionability* [applicability, or practicability], or knowledge hierarchy is exhibited in *Figure 1*.

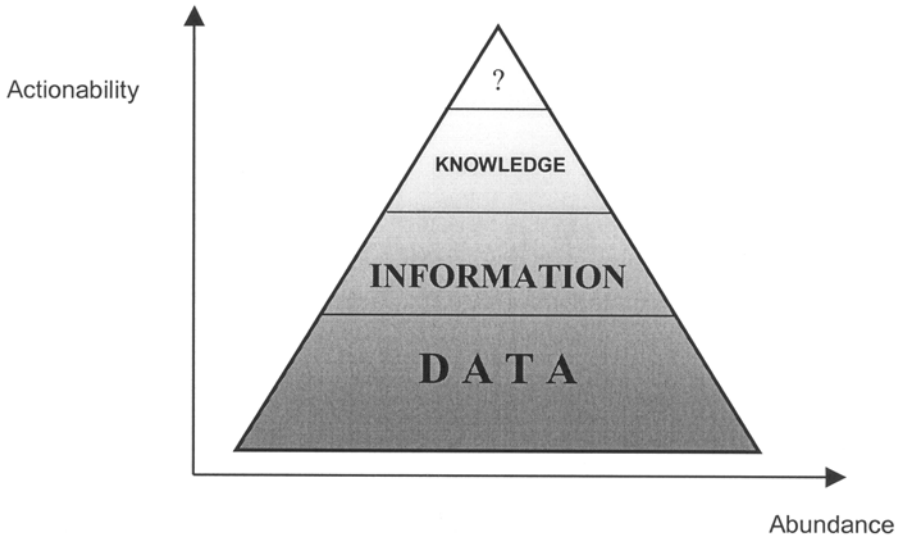


Figure 1. Knowledge Hierarchy

The correlation of the three layers, data, information, and knowledge is as follows: Data become information when the receiver adds meaning to it. Information becomes knowledge when it is applied, or when an action, based upon information, occurs.

Knowledge lies in the "hierarchical pyramid" above information and data. However, most information technology (IT) employed in order to manage knowledge appears to target data and information rather than knowledge itself (e.g. Ruggles 1997). Moreover, existing IT is oriented primarily at database management systems (DBMS), data warehouses, data mining (DW/DM), Internet/intranets and groupware (O'Leary 1998). Extant IT provides, at a maximum of its ability, only common, machine-dependent means for the management and distribution of information, not knowledge.

For example, one can see that data mining applications are mostly associated with sophisticated data pattern matching. Databases and indexing help structure data and information. Groupware and search engines are mostly related to distribution of information. However, the actual ability to build knowledge upon such data and information still remains highly individualized.

2. Knowledge Management and Knowledge Flow

The power of knowledge has been acknowledged for hundreds of years. However, today it is recognized more at the enterprise level rather than at the level of successful individuals. Studies of prominent technology firms showed that knowledge has become the key economic resource and dominant source of comparative advantage in the market competition (Drucker 1995, and others). Such "corporate" knowledge is denoted as *knowledge management* (Davenport and Prusak 1998). Although the definitions of knowledge management vary (see for example Leibowitz's summary 1999), they share similar key points—knowledge must be systematically built and applied to fulfill organization objectives, enhance collaboration, support innovation, and magnify performance. Commonly, knowledge management means "to get the right knowledge to the right people at the right time to allow the right decisions."

Knowledge can generate innovation, and an organization can obtain a competitive edge through such innovation (Davenport and Prusak 1998). But, to posses the competitive advantage, knowledge must be not only created but also transferred and used throughout the whole organization. Such movement is called *knowledge flow*. It is obvious, for the military, that knowledge flow is imperative. However, the phenomenon of knowledge flow is not properly understood, and the benefits of theory of knowledge management and its application are not fully employed.

The mechanics of knowledge flow between two *nodes*, or *agents*, in the organizational structure—no matter whether the nodes are people or machines—is quite similar to inter-computer data flow through several layers of hardware and software. The flow starts at the knowledge level and descends through information to data in one agent. The data are then transmitted via certain media (e.g. a computer network) and flow to the other agent. Then the flow ascends in the reverse order through information to knowledge (Nissen 2001).

This notion of *layered processing for knowledge flow* has brought some very important insights:

- In this concept, machines, such as computers, expert systems, and intelligent agents, and people, as individuals, in groups, or in organizations, exchange knowledge via layers of information and data in a similar fashion.
- Direct transfer of knowledge or information is not possible because the exchange always occurs at the data level. Implicitly, if knowledge is to be transferred between different agents, the agents must be able to send and to receive data, upon which the knowledge is based.
- To comprehend knowledge flow, one must understand the processing used by various agents (again, human or machine) to transform data and information into actionable knowledge, and vice versa.
- The abstract and "intangible" concept of knowledge can be turned into an observable and measurable action—thus allow differentiating the knowledge of various agents based on their relative performance.

The primary objective of knowledge flow is "to enable the transfer of capability and expertise from where it resides to where it is needed—across space, time, and organizations as necessary." (Nissen 2001, p. 1) Studying knowledge management and knowledge flow in its complexity, researchers Nissen, Kamel, and Sengupta described the cyclical flow of knowledge in its complexity by developing the *Knowledge Management Life Cycle* (KMLC).

3. Knowledge Management Life Cycle

Knowledge management has been investigated for many years. Different authors were describing knowledge and knowledge management, mostly concentrating on how knowledge is captured and shared. A comprehensive view was missing until Nissen et al. (2000) presented a life cycle associated with knowledge management. Their amalgamated model of KMLC is depicted in *Figure 2*.

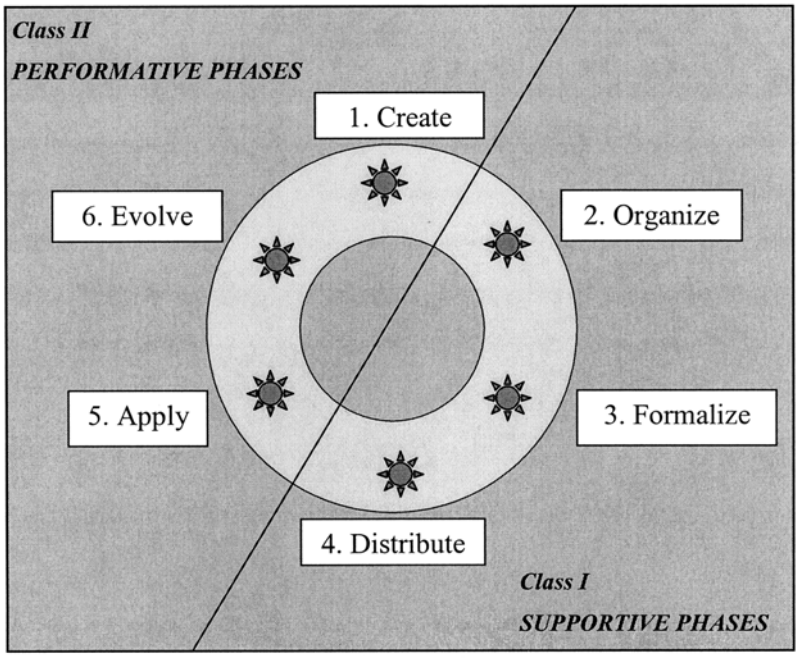


Figure 2. Knowledge Management Life Cycle

As exhibited in the figure, the KMLC is divided into six phases and two classes: *Creation* of knowledge occurs primarily in the minds of individuals. This creation encompasses the discovery and the development of new knowledge (Gartner Group 1998). Such knowledge is tacit, unstructured and external to the organization (Nonaka 1994). In the second phase, which definitely pertains to the organization, knowledge is *organized*. It is mapped, or bundled, so that the organization can recognize it. Then, in the phase of *formalization*, such knowledge is to be transposed from its tacit to its explicit form. Now, knowledge is structured and internal to the organization. Once formalized, knowledge is *distributed* throughout the organization in order to be shared among its members. This phase, heavily supported by existing IT tools, is currently the most emphasized phase. Knowledge, after that, can be *applied,* or used for problem solving or for decision-making processes. Finally, knowledge can further *evolve*, meaning that it can be refined and continually developed. Moreover, the evolution of knowledge can lead to the creation of new knowledge, thus to the generation of a new KMLC.

When comparing the six phases of the KMLC, Nissen et al. noted that extant systems and practices support the process of knowledge management unevenly. Especially at the organizational level, they mostly support knowledge organization, formalization, and distribution, i.e. the phases grouped in *Class I*. This class is inherently *supportive* to people in the organization because it supports people in the enterprise, whom in turn apply, evolve and create knowledge in the organization. Class I systems are known as *localized management systems*, represented by tools such as knowledge maps, "yellow pages," distributed lessons learned, and others. Obversely, the phases from *Class II* are not well supported by existing IT. They are innately *performative* in nature because they perform knowledge-management activities, either in combination with or instead of people in the organization.

Researchers (e.g. Nissen et al 2000) have shown that the knowledge flow has not been fully explored yet, especially in terms of integrating the knowledge *process design* with the knowledge *system design*. Yet they concluded that the current set of methodologies used in reengineering, expert systems, and information systems provide capabilities to design and develop IT, which is necessary for knowledge management

systems and processes. Furthermore, the researchers stressed that no single methodology is sufficient to develop all knowledge management systems and processes; a multiple developmental approach is essential. Such approach is represented by the *knowledge system and process design*.

4. Knowledge System and Process Design

As IT has become more and more present in our daily lives many enterprises and governmental organizations view it as a magic tool that could improve performance dramatically. Indeed, computer networks can create an infrastructure requisite for knowledge exchange, but reality proved many times that a simple insertion of IT into existing processes does not provide a warranty for the desired improvement. As noted by Weber (1993), IT provides only a temporary competitive advantage; it is just "self-canceling technological advantage." Contrary to material assets knowledge can grant sustainable advantage because it generates increasing returns—knowledge assets increase with use (Davenport and Prusak 1998).

Nissen and other researchers have revealed that information technology must be integrated with the design of the process it supports—including the organization, people, procedures, organizational culture, and so on. They identified two *contextual factors* that define and limit knowledge management systems design: the *organization*, and the *nature of knowledge underlying the task* (Nissen et al. 2000).

When considering the first contextual factor, an organization, attention should be paid to these aspects:

- *Not everything that occurs is recorded*: An organization has memory systems that maintain the lessons learned from experience (Levitt and March 1988). The knowledge resident in an organization's memory establishes a mechanism for conserving its history, routines and the lessons learned over time. As outlined, these memory elements can be recorded in many ways, formally as

well as informally. However, no organization can currently record all of the existing memory elements.

- *Essential aspects of knowledge reside in the informal state*: Knowledge captured via informal mechanisms is often richer and more important than what is stored formally. So the key to building useful knowledge management systems lies in solutions that can capture the essence of informal knowledge in a shape that can be preserved. Such knowledge, once lost, cannot be re-created easily (Hutchins 1991). When, for example, a member separates from the organization, the potential for loss of knowledge is ample, especially in cases when locating existing knowledge in time and transferring it to where it is essential is troublesome.
- *The structure of the organization significantly influences the practice of knowledge creation, storage, and dissemination*: Conventional organization structures rely more on informal networks and communities, and have well-developed channels and norms for communication. Modified organizational forms enabled by information technology, such as virtual and networked organizations, are typically ad hoc in nature and must form such channels first. Moreover, maintaining continuity is difficult, and the history of relevant organizational knowledge is not easily available.
- *Retention and updating of knowledge is mostly an upstream activity while the benefits from its dissemination and use go downstream*: (Davenport and Prusak 1998, Grudin 1996) This contraposition creates specific problems. The decision is often made on the basis of managerial factors, such as cost and schedule. Because capture of knowledge can add to the cost and cause time delays, high proportions of projects are terminated before they are completed. Also, the benefits of the knowledge are usually accrued in the latest stages of the project and many times by different people. Thus focusing only to technical aspects of knowledge management applications is insufficient. Such systems can only prosper if appropriate incentives for the retention and updating of knowledge are provided.

The nature of knowledge underlying the task, the second contextual factor, defines and limits knowledge management systems design in the following ways:

- *Hierarchical practices, such as manuals and job descriptions, frequently used to organize the processes are usually inadequate for complex problems*: That is because the effort involved in acquiring knowledge required to perform a complex task effectively is not negligible (Lave 1988, Lave and Wenger 1990), and because the knowledge acquired and represented in the canonical methods can become obsolete with changes in the task-related technology (Suchman 1987).
- *The actual approach to complex problems solving often departs from the prescriptive methods*: Individuals performing complex tasks may improvise, resorting for non-orthodox practices to overcome shortages of hierarchical approaches. (Zuboff 1988) These non-formulary practices can serve as extensions of canonical methods, compensating for the omissions and inadequacies of prescriptive knowledge. Such practices can also modify the hierarchical methods, once they seem obsolete or less effective than the corresponding methods used in practice.

When studying the knowledge management, researchers Nissen, Kamel, and Sengupta focused on knowledge management from three integrating angles: reengineering process innovation, expert systems knowledge acquisition and representation, and information systems analysis and design. They coordinated these three perspectives into one complex design approach, which starts with the analysis and design of the organizational interest, continues with the knowledge capture and formalization, and ends with the system design and implementation. Their design process is referred to as the *knowledge system and process design.*

According to the researchers' study, the knowledge system and process design should follow four stages (Nissen et al. 2000, Nissen 2001):

(1) *Process Analysis*: The first stage requires understanding the objectives and strategies of an organization. Without understanding the process (including different variations) and required knowledge, there is no use to begin

designing the system. The aim here is to define the knowledge ensuring effective performance of each process of interest. Canonical practices might be of help but a "hands-on" approach is also needed.

(2) *Knowledge Analysis*: This analysis results from the previous analysis and concentrates on identifying and analyzing the knowledge within an organization. Central to this step is identification and analysis of *critical success factors* (CSFs)—activities that must be performed effectively in order for the mission to be successful. CSFs are useful to identify what knowledge is crucial to process performance in a particular organizational setting and context.

(3) *Contextual Analysis*: In this phase, knowledge itself should be captured, particularly the tacit knowledge used by specialists. Databases, intranet applications, and search and retrieval systems can be used to organize, to formalize, and to distribute the captured knowledge. "Yellow pages" and knowledge maps, when available, can help identify who possesses what kind of knowledge. Understanding the organization and the nature of knowledge is essential in this assessment.

(4) *Systems Analysis and Integration*: In this final stage, the organization's current procedures and information systems are analyzed. Also, any methodologies, techniques, and tools that are available and are understood can be employed to develop a knowledge management system. Information systems required to automate and support knowledge work can then be effectively designed.

Knowledge itself seems to be difficult to manage and is resistant to reengineering and process innovation (Davenport 1995). The key point is that all three "facets"—*process*, *knowledge*, and *information*—should be considered together when designing knowledge systems and processes (Nissen et al 2000). Abrupt implementations of "IT solutions" into existing processes and organizations without having considered all key factors helps little.

As expressed before, knowledge management is essential for an organization striving for a competitive advantage. Certainly knowledge management represents

a significant challenge in such a complicated and large "enterprise" as a military. Yet, effective knowledge management is vital for the military domain that is solely based upon knowledge—military intelligence.

B. INTELLIGENCE AND MILITARY INTELLIGENCE

Since the end of the Cold War, many nations, including the Czech Republic, have found their security less threatened. Thus the focus of national security has changed, but the mission of the military intelligence community remains the same: to provide timely assessed intelligence for military commanders and to support military operations.

Initially this section presents some basic information related to intelligence, as a foundation for further analysis. As military intelligence is just a more specific subset of intelligence, most of the general facts about intelligence also apply to military intelligence.

1. Intelligence Functions and Intelligence Disciplines

As the term "intelligence" is used in numerous ways, defining the term is essential. In terms of national security, intelligence, as it is more or less unanimously defined, can be seen as:

- A *process* during which required information is collected, processed, analyzed, and disseminated to the customers of final intelligence. In other words, intelligence is a process that converts raw data into a solid product, which satisfies the needs of those to whom it is concerned.
- A *product* representing the result of the intelligence process.
- An *organization* or an *agency*, which actually conducts some or all of the intelligence functions.

Many people assume that the main task of an intelligence service is to describe the truth about something in reality. As Lowenthal (2000) explains, intelligence is not

about truth. If something were known to be true, states would not need intelligence services to collect or to analyze the information about these facts. The requirement to always discover the truth would set a standard that no intelligence agency could achieve. Thinking of intelligence as a matter of describing approximate reality is more accurate. Intelligence tries to understand what is occurring in any given issue and tries to produce reliable, unbiased, and honest (i.e. objective and non-politicized) intelligence.

So, why do we have intelligence agencies? Intelligence should exist solely to support decision-makers. To allow better decisions, intelligence agencies must provide decision-makers with accurate, timely, and tailored intelligence. This is true for every intelligence service—be it a national foreign intelligence service, a military intelligence agency at the strategic level, or a military intelligence unit on the battlefield. Any motive other than supporting decision-makers would be wasteful or even illegal. According to Lowenthal (2000) intelligence services exist for at least four reasons:

(1) *To Avoid Strategic Surprise*: The leading goal of any intelligence service must be to monitor threats, troops, and events that can potentially jeopardize the nation's existence.

(2) *To Provide Long-term Expertise*: As policy makers come and go, being versed in all the national security issues with which they deal is impossible. They need intelligence personnel with extensive expertise and knowledge on many subjects. The intelligence community has a relatively stable analytical staff, and it tends to have fewer political appointees than other elements of the state bureaucracy.

(3) *To Support the Policy Process*: Policy makers constantly need tailored and timely intelligence that will provide background information and warnings. Intelligence agencies can prepare such information and assess the risks and benefits of the steps the policy makers intend to take.

(4) *To Maintain the Secrecy of Information, Needs, and Methods*: Since adversaries and competitors withhold information, and since we also want to keep specific information secret, each nation must possess effective intelligence services. With such services, a nation has the means for collecting

and processing information about other potentially hostile nations while guarding its own sensitive information against the adversary nations.

The complexity of all the functions listed above, coupled with the development of the technical means for collecting information, has led to a specialization in intelligence gathering. Hence separate, yet interconnected, *intelligence disciplines* have been created. Realistically, no single individual or organization can efficiently and accurately collect and process all the available information, and this fact has generated a need for intelligence specialization. Furthermore, considering the impact of IT on today's society, further specialization will likely occur.

Over the past four decades, NATO intelligence disciplines have evolved and have been categorized into five main categories:

- *Human Intelligence* (HUMINT);
- *Signal Intelligence* (SIGINT), which has two subcategories:
 - *Communication Intelligence* (COMINT), and
 - *Electronic Intelligence* (ELINT);
- *Measurement and Signature Intelligence* (MASINT);[1]
- *Imagery Intelligence* (IMINT);
- *Open-Source Intelligence* (OSINT).

Obviously, HUMINT represents human, non-technical discipline while SIGINT, IMINT, and MASINT are mostly technical. OSINT comprises both human and technical approaches.

2. Intelligence Process and Intelligence Cycle

This section concentrates on intelligence as a process. According to current definitions,[2] intelligence as a process involves requests for the collection and analysis of

[1] This discipline is recognized only by the US intelligence. Other nations do not use this category as a separate intelligence discipline. Also, this category is not included in NATO allied doctrines, such as AJP-2.0. (2001)

specific types of information, and then provides the finished intelligence to decision-makers. In these terms, the intelligence process should be understood as a set of interrelated steps, transforming raw information into a finished intelligence product. To describe the entire process, the intelligence community uses a model called the intelligence cycle.

Most publications (e.g. AJP-2.0. 2001, FAS 1996) describe the intelligence cycle as both separated, and yet inter-connected, components of direction, collection, processing, analysis and production, and dissemination. To this, Lowenthal (2000, pp. 50-51) presents his more explicit model, which also contains consumption and feedback. To better describe the complexity of the intelligence process graphically, the author created an amended model of the intelligence cycle. The model is depicted in *Figure 3*.

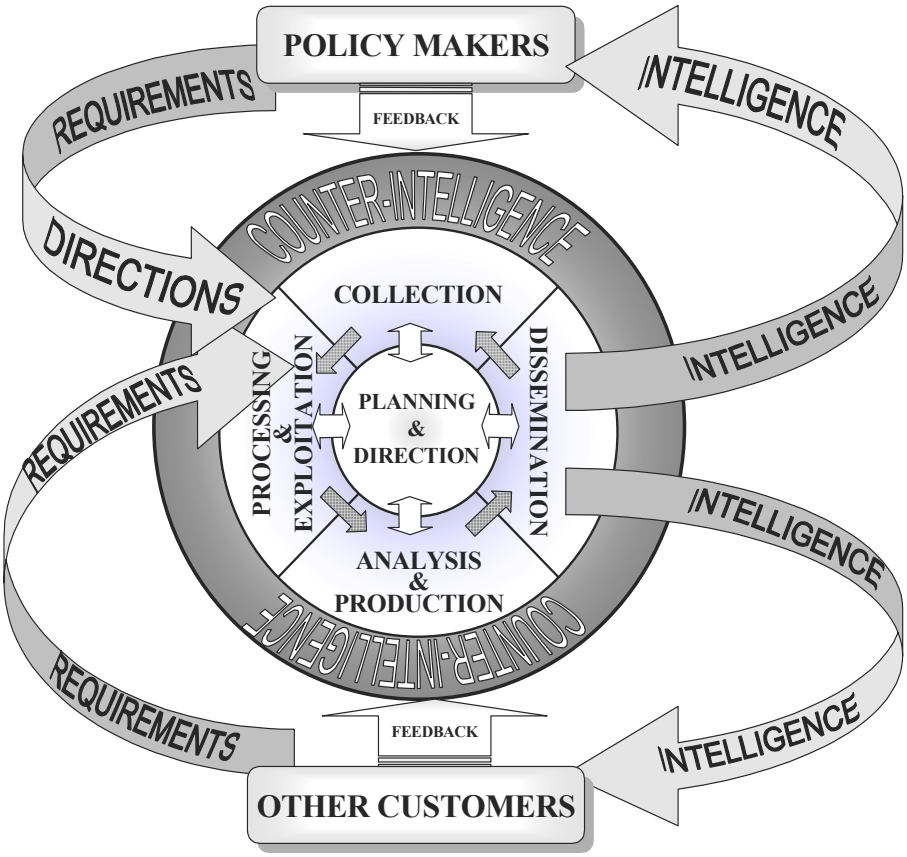


Figure 3. Amended Model of the Intelligence Cycle

2 See for example: AJP-2.0. 2001, p. 1-2-3 or Lowenthal 2000, p. 8.

The intelligence process, by nature, is rather continuous. The intelligence cycle has no specific or definite beginning or ending. Intelligence operates in an environment with erratic information, changing requirements, and unending analyses. However, the following separable components of the intelligence process have been determined:

Planning and Direction: In the amended model presented in Figure 3, planning and direction are in the center as the core elements of the intelligence process. Intelligence organizations are predominatingly bureaucratic in nature, so planning and direction is vital to keep them effective. Moreover, as the intelligence budgets and manpower decrease and possible threats become more scattered, intelligence must be oriented toward the stated or implied needs of its customers.

Planning and direction emanates outside the intelligence agency, but is also necessary inside the organization itself. As decision-makers pose their tasks and questions, an intelligence agency further specifies, analyzes, and refines the requirements to ensure that:

- The intelligence organization comprehends the requirements;
- The tasking authority understands the capability of the agency;
- The available collection assets will be properly tasked in accordance with the intelligence requirements.

Rather than seeing planning and direction as only the first phase of the intelligence cycle, one should understand it as a core element that receives tasks, sends commands and collects feedback almost continuously.

Collection: Collection is the actual gathering of information needed to produce the finished intelligence. Intelligence assets collect information using different sources and methods, generally referred to as "intelligence disciplines." The five collection disciplines, HUMINT, SIGINT, MASINT, IMINT, and OSINT, were already introduced in the previous section.

Collection assets gather information, in accordance with plans and procedures, to fill the gap between what is already known and what must be known in order to answer the consumers' questions and to fulfill the tasks assigned to the intelligence agency.

Processing and Exploitation: This phase fulfills a dual function in that the collected data and information are usually processed and then exploited for further analysis. This is especially common for the technical intelligence disciplines where data does not arrive in ready-to-use form. *Processing* converts the collected signals into images or other forms. In *exploitation*, analysts transfer the data and information into a more usable form through decryption, language translation, data reduction, and so on.

Analysis and Production: Information is seldom usable in its raw form. Therefore, it must be analyzed. Furthermore, information can often be fragmentary and even contradictory. During the analysis, new value is added through *collation*, *evaluation*, *analysis* and *integration*, and *interpretation*. An analyst constructs a coherent picture of the evaluated information and produces the finished intelligence product that assesses events, judges possible implications and estimates further development.

Dissemination: If the finished intelligence is not delivered to its intended recipients, it has zero value regardless of its quality. Thus dissemination is an equally important part of the intelligence cycle. The finished intelligence must be distributed in an accurate, complete, yet concise and timely fashion, and it must satisfy the customers' needs.

Counter-intelligence: The amended model sees counter-intelligence as an envelope protecting the entire intelligence process. Moreover, counter-intelligence should also protect the distinct parts of the intelligence cycle separately. However, one should consider that the counter-intelligence process moves through the same cycle as depicted in Figure 3.

Consumption: Lowenthal includes "consumption" among the intelligence cycle steps. This thesis considers consumption as an interaction with intelligence, rather than as one particular step in the intelligence cycle itself. As mentioned before, intelligence products are intended to help decision-makers take an action. But, as Lowenthal points

out, “policy makers are free to reject or to ignore the intelligence they are offered.” (Lowenthal 2000, p. 8) An intelligence organization cannot compel its customers to use its product—it can only do the best to meet the customers’ needs.

Feedback: Feedback is rarely seen in the intelligence community. This is reflected in many different models (e.g. AJP-2.0. 2001, FAS 1996), in which feedback is not even mentioned. As Lowenthal (2000) stressed, ideally the community would receive information about whether its product has been useful or not, about which areas of interest require increased attention, and so on. But in reality such feedback is rarely received. This lowers the effectiveness of the intelligence process.

However, feedback can be considered as information flowing in an opposite direction throughout the intelligence cycle—as a tool beneficial to the community rather than as a separate component of the cycle itself.

3. Common Problems and Challenges in Intelligence

Now, before entering the specifics of OSINT, some of the problems and challenges prevalent in intelligence will be discussed. Understanding the nature and causes of such challenges will establish a firm basis for the analyses in later chapters.

Intelligence as a very old and frequently used tool of statecraft faces many difficulties. Some of the intelligence requirements have significantly changed over time while others remain almost constant. Here is an overview of main issues in contemporary intelligence:

Intelligence Requirements: The current international situation is in many ways more complex and more difficult than the relatively "stable" bipolar Cold War. The absence of one or a few overwhelming intelligence requirements has been replaced by many new requirements, none of which has the same lasting importance. Unlike twelve years ago, nowadays intelligence issues are of the highest priority for rather short periods

of time. At the same time, the human and budget resources available to the intelligence community continue to decline in many countries.

The U.S. Ambassador Robert Kimmitt, former Under Secretary of State for Political Affairs, once stated that the intelligence community "will have to be an inch deep and a mile wide, with the ability to go a mile deep on any given issue." No longer is there just one enemy creating one global nuclear threat—nowadays, there are many "newcomers" at play. Not only military personnel, installations or units, but also paramilitary and civilian organizations and individuals have gained the attention of the military intelligence. Rogue non-state actors, such as terrorists, ethnic extremists, and religious fanatics—all potential users of proliferation of weapons of mass destruction (WMD)—rapidly increase the demand for intelligence supporting efforts (Tenet 2000).

Today's electronic environment complicates the situation even more, allowing possible adversaries to act more effectively than before because interconnectivity has become global.

Value and Vulnerability of Information: The information revolution has not been an easy transition from a person-to-person type of society to a global-information-network society. Yet, today's information is equivalent to the information gathered a few centuries ago in terms of its importance. The propagation of satellites, massive databases, cellular phones, fax machines, and computer networks created a new dimension in the intelligence environment.

In the electronically interconnected world, information moves at the speed of light, is nonmaterial, and is of enormous value—hence information itself has become a vital strategic resource (Schwartau 1996). On one side, information is now considerably more vulnerable; on the other side, it can be used with surprising effectiveness. Information that leads to correct decisions and wins the battle is a weapon in itself.

Secrecy versus Openness: A vast amount of information is available from open sources. But we still need to gain information that our potential adversaries conceal while sufficiently protecting our own intelligence. Of course, existing and rising democracies seek as much openness and freedom of information as possible.

Knowledge often equates to power, so there will always be a tendency to keep at least some knowledge confidential. And some people will always want to acquire knowledge for their own use—for reasons that could be selfish, unethical, or even criminal. We are unable to change this situation today. As long as information can be kept secret or can be misused, such a situation prevails.

However, it should be understood that intelligence need not be only about secrets. Definitely, intelligence collection has two facets—*open* and *covert*. Each side has its own importance and should be effectively employed and managed. But in practice, many segments of the intelligence community undervalue open-source intelligence.

Intelligence "Stovepipes": Two characteristics related to intelligence disciplines are frequently denoted as intelligence "stovepipes." The first characteristic is that all disciplines but OSINT have end-to-end processes, from collection to dissemination. The second characteristic is that the intelligence disciplines are practically separated from one another, being competitors for various reasons. Thus intelligence disciplines are often visualized as distinct "pipelines" or "stovepipes"—complete, yet completely individual and separate processes.

The five intelligence disciplines, HUMINT, SIGINT, MASINT, IMINT, and OSINT, have not developed evenly throughout NATO, and as a result, intelligence agencies do not manage them in similar manners. Each discipline has particular strengths and weaknesses, one working better or worse than the other in specific intelligence tasks. This situation stems from the Cold War when intelligence was more linear and oriented in one direction. Today, a number of individual organizations perform distinct missions and yet support an overlapping set of customers. Furthermore, these organizations have become competitors for resources. All of this regularly complicates the decisions about overall collection needs and resources.

Physical Capabilities and Limitations of an Intelligence Analyst: Especially in the technical categories of intelligence, not all of the collected data are exploited and processed. The future development of sensors and advanced communication will increase that amount of unprocessed information, thus contributing to the all-source analysts'

workload. Today, intelligence is becoming based on real-time demands, and intelligence consumers sometimes expect immediate answers while the intelligence analysts can offer only tentative analytical estimates.

Information Overload: Widespread information technology and electronic communication has also created very specific problems in the intelligence community. On one hand, a vast amount of information is readily available and can be collected by all sorts of reconnaissance and intelligence assets. On the other hand, this availability creates an enormously high demand for analyses, processing, and dissemination of intelligence.

Although the technical collection disciplines radically improved in terms of gaining information, this improved ability also inundates agencies with too much information. As the power of computers doubles every 18 to 24 months (Moore's law), working with information and building knowledge has become the key for gaining the competitive advantage. How do we decide what information we need? Can we make rational, well-informed decisions about which information is truly valuable or which piece of information is even reliable?

Today, the emphasis is still placed more on processing masses of information rather than on identifying and structuring information according to its likely utility. Unstructured information of all kinds is widely dispersed not only throughout the intelligence agencies, but also throughout different non-military organizations. For example, shortly after the terrorist attack on September 11, 2001, many journalists quickly obtained information that had been available prior to that terrifying date. But different elements of the data were spread throughout different agencies, and no person, organization or momentum was able to connect the whole puzzle that would prompt the requisite countermeasures.

Information management is definitely an extraordinarily demanding task, but knowledge management is an even more crucial element to explore.

Knowledge Management and Intelligence: In the corporate world, the growing importance of professional knowledge work has been reflected in the rapidly increased employment of computer and communication technologies. This has also been reflected

in the newly created managerial posts—such as "Chief Information Officer" (CIO) or "Chief Knowledge Officer" (CKO). The military services have also recognized the emerging importance of knowledge management. Not unlike the civilian sector, knowledge management has become a fad to many—and a nightmare to others. No wonder that in many cases, the design or reengineering of information systems did not follow the four-step procedure of the knowledge system and process design described before. Many systems, experimenting with software applications without a scientific basis, have been built by trial and error.

Certainly, managing knowledge in such large and complex organizations as in the case of the military is quite difficult. With intelligence, the situation is even more problematic because all the services have developed their intelligence elements at different command and control levels. Furthermore, intelligence disciplines have not developed consistently throughout the intelligence community.

Today, a more dynamic military environment creates more changes in the presence of military personnel in the battlefield. Examples from operations in Persian Gulf, Bosnia, and Kosovo showed that the rotation of personnel, for example, causes obvious losses of knowledge that were previously gained. Understanding various actions and events in the operational theater requires considerable time, and such knowledge has been hard to capture and to formalize for further use.

C. OPEN-SOURCE INTELLIGENCE (OSINT)

This section briefly examines some aspects of open-source intelligence (OSINT). After open sources and OSINT are defined and categorized, the basic principles and current problems and challenges of OSINT are presented.

1. Definitions and Categories

Open sources are unclassified sources of information in the public domain or available from commercial services (Denning 1999, Lowenthal 2000). They can be gained in various forms:

- *Printed Publications*, such as newspapers, magazines, journals, books, reports, conference proceedings, and manuals;
- *Broadcast Services*, such as radio and television;
- *Electronic Resources*, such as off-line and on-line information databases, the Internet, and multimedia CDs;
- *Public Demonstrations*, such as speeches, hearings, press conferences, symposia, and trade shows;
- *Conversation* with scholars, experts, and event participants.

Categories of Open Sources: Open sources are categorized according to their media, on-line or off-line accessibility, costs, and so on. This thesis classifies open sources as follows (NOSINTH 2001, OSINTH 1997, and others):

- *Traditional Media Sources*: This category encompasses domestic and foreign print and broadcast media, radio and TV, as well as electronically available products. Media sources still remain the core of OSINT. The US Foreign Broadcast Service (FBIS) and the British Broadcasting Corporation (BBC) Monitoring Service are considered excellent examples of media sources.
- *Internet*: The Internet is mostly used for Web browsing and e-mail, but it provides an array of other services—electronic conferences, news groups, and also provides direct access to a growing number of specialized databases. In fact, the Internet has become the communication backbone of the commercial world.
- *Commercial Online Premium Sources*: These sources are usually civilian commercial organizations charging a subscription fee or a usage fee for online access to their information. Many of these sources represent years of work on specific subjects, offering validated information, indexes, abstracts, and so on. Such services can also be obtained through information brokers or professional librarians. Frequently cited examples of commercial online premium services are LEXIS-NEXIS, FACTIVA, and DIALOG.
- *Other Commercial Sources*: This category includes professional services available through direct subscription, both on the Internet and in the form of

hardcopy or CD-ROM publications. Many of the services are directly oriented to areas of military interest. For example, The British Library monitors international publications and conferences about many general topics, including military matters, and produces excellent proceedings; Orders of Battle, Inc. offers complete orders of battle of 188 countries.[3]

- *Gray Literature*: Gray literature refers to public non-proprietary documents that are available in very limited numbers and are mostly accessible only inside the country of publication. This category encapsulates working papers, technical reports and blueprints, pre-prints, and so on. Gray literature, positioned between online information and human expertise, contains an important collection of knowledge.
- *Commercial Imagery*: Overhead imagery is no longer solely a military domain. In recent years, commercial industry gained significant capabilities, such as high-resolution electro-optical imagery, useful especially for multi-national joint combined military operations. For example, SPOT Image offers various products ranging from digital geospatial data, to overhead imagery, radar imagery, natural hazard assessment, evaluated image maps and 3-D terrain mapping.
- *Overt Human Experts and Observers*: For many topics finding exactly what is needed is hard. Moreover, both electronic and printed public information is scarce for many countries. In all cases, an expert or an observer with direct experience represents the ultimate open source. First, internal subject-matter experts who are scattered across various elements of the organizational structure can be found within the military organization. Second, based on their accomplishments and publications, outside experts can be located. Finally, "local knowledge" experts, such as frequent travelers, local residents, and event participants, can frequently provide deep insights into specific conditions.

[3] Actual numbers may vary. See http://www.orbat.com.

The above categories are not intended as strict divisions and may overlap to some degree. They are mentioned here merely to provide a sketch of open sources.

Open-Source Services: Aside from the information provided, many commercial sites also offer extended services associated with open sources. Such services vary, but they generally fall onto the following three categories (NOSINTH 2001):

- *Collection Services*: Collection services include online data collections by specialized researchers, off-line acquisition of documents or gray literature, different forms of surveys and polling, private investigations, aerial surveillance, and so on. Many essential documents can be gained through private-sector organizations that are established worldwide.
- *Processing Services*: This category embodies data conversion, indexing and abstracting, interpretation of imagery or signals, translations from foreign languages, database creation, and other similar services.
- *Analysis and Production Services*: Individual experts and commercial and academic organizations can be hired to analyze and produce various services, especially when the topic requires high expertise or the topic is out of reach of one's organization. Outsourcing may deliver excellent results if real experts are employed.

OSINT: Similarly to the other intelligence disciplines, OSINT involves much more than just collection; it goes through all the phases as described in the intelligence cycle. So, processing and analyzing the collected open-source information adds value. Open-source intelligence, like any other discipline, requires humans—to exploit the information, to sort the important from the unimportant, to retrieve relevant knowledge, and to judge the reliability of the source.

The NATO Allied Joint Intelligence, Counter-Intelligence and Security Doctrine (AJP-2.0. 2001) defines OSINT as "Intelligence derived from a wide range of open sources such as radio, television, newspapers, and books to which the public has access." The NATO Open-Source Intelligence Handbook (NOSINTH 2001) further divides intelligence emanating from open sources into two distinct categories:

- *Open-Source Intelligence* (OSINT): OSINT applies the proven model of the intelligence cycle to the broad diversity of open-source information and creates intelligence products;
- *Validated Open-Source Intelligence* (V-OSINT): V-OSINT possesses a very high degree of certainty. It can be produced by all-source professionals with access to classified information, or it can originate from trusted open sources whose validity is without question.

2. Problems and Challenges in Open-Source Intelligence

OSINT, as one of the intelligence disciplines, bears some of the general problems of intelligence "business"; OSINT also carries some specific problems not seen in other disciplines. In this section, some of the prevailing problems and challenges in OSINT will be discussed.

Use of Open Sources: During the Cold War, at least 20% of the information contained in intelligence reports came from the public domain. Today, in light of the greater openness of governments around the world, that figure can be as high as 95% (Johnson 2000). Although the percentage varies with the originator—starting as low as 40% (CIA), OSINT clearly plays an important role in intelligence.[4]

Certainly, open sources could replace pure field intelligence in many areas, or at least could compete sufficiently.[5] Keenan (1997) projected that up to 95% of what the US government needs to know could be acquired through a careful and competent study of open-source information that exists within the country. Indeed, in this area the United States has attained a high level of success. But many other countries, including the Czech

[4] Here is a true story: When NATO decided to bomb targets in Kosovo, many European countries had their intelligence agencies on stand-by alert. One nameless intelligence team, tasked to report when the mission would start, received this advice from the supervisor: “Switch-on the TV and watch CNN!”

[5] See, for example: A story about British intelligence using mainly open sources during the Falklands War (Adams 2000, p. 225). Another example is a "contest" between Robert Steele and CIA to obtain a complete intelligence report on the African nation of Burundi over a three-day period (Denning 1999, p. 80).

Republic, can also gain a significant portion of their needed information from their open sources and from sources abroad.

However, OSINT should not be the only intelligence collection discipline used to provide accurate intelligence. OSINT can serve as the first resource for any intelligence analysis—but cannot replace the other disciplines in full. Clandestine collection and information operations cannot be omitted; in some cases they can "make the difference between life and death on the battlefield or between an aborted and a tragic terrorist incident." (Denning 1999, p. 81) For this reason, there should be no competition between OSINT and other disciplines. Instead, OSINT should serve as a broad base for the other intelligence disciplines in which intelligence must be collected by other than overt means.

OSINT is vital to the all-source intelligence analysts because "it provides the historical background information, the political, economic, social, demographic, technical, natural, and geographic context for operations, critical personality information, and access to a wide variety of tactically useful information about infrastructure, terrain and indigenous matters." (NOSINTH 2001) For most cases, OSINT can really serve as a foundation for constructing the whole intelligence picture—principally when the military must understand its involvement in non-traditional tasks, such as ethnic and religious conflicts, clashes for scarce natural resources, mass migrations, natural and technical disasters, international organized crime, and so on.

OSINT can contribute to classified collection methods in the following areas:

- *Tip-offs*: Electronic media, the Internet in particular, provide vast opportunities for information exchange. As a result, the number of areas with denied access to information has diminished since the end of the Cold War. Today, many services provide non-traditional news alerts, witnesses post their messages on the Internet newsgroups, and so on. Hence, there are many situations where OSINT can provide the first indication of an event—even before it is covered by the media such as CNN.
- *Targeting*: Both OSINT and classified sources can be optimized for a particular intelligence problem. This allows intelligence personnel to concentrate on issues that can only be discovered covertly and also to validate the OSINT products via the classified collection. Thus, OSINT optimized with

collection from other sources allows all-source analysts to work more effectively.

- *Validation*: Classified reports are often narrowly focused and represent separate pieces of intelligence. To counter the preoccupation with only one direction, one can place such reports into a wider context, supplementing necessary background information from the OSINT environment. Cross checking such intelligence through multiple open sources can assure its validity.
- *Cover*: In some instances, open sources can serve as a plausible cover for the sanitation of classified reporting. If one understands the information available in unclassified systems, the ability to use a plausible alternate open source as a cover is facilitated. Thus, open sources can serve as a shield that can conceal the real source of the information.

Misconceptions: Theoretically, the greater availability of open sources should ease the task of the intelligence. However, intelligence services were created to collect secrets—and using open-source information seems not congruent to the task at hand. That is probably why intelligence agencies have difficulties assimilating open sources into their processes. Intelligence services often do not want to confess that much of their work is based on open sources. Many intelligence agencies will not admit that they rely on OSINT heavily because they fear that their budgets will be severely cut, that they will lose professional respect, or even that their departments will be eliminated. They assume that most taxpayers might ask, "Why do I have to pay for an intelligence agency that reads the newspaper?" Some people mistakenly equate the value of intelligence with the degree of difficulty involved in obtaining it and with the classification level assigned to it.

Another common misconception about OSINT is that it can be obtained without cost. But one can easily understand that gaining information from open sources is subject to direct and indirect costs. Direct costs include the cost of printed materials, the fees for subscription to electronic resources, the expense for experts from outside the organization, and so on. Indirect costs include, for example, expenditures for supporting

IT tools, paying analysts inside the organization, and opportunity costs. However while open-source information is not free, the associated costs are often far less than those of collecting and processing classified information.

Another misunderstanding is that the Internet is the primary origin of most OSINT. Indeed, the Internet has about 500 million users and is increasingly used as a means of open-source collection that holds about one billion documents, many of which are linked. Expert forums, including private teams with their own newsletters and e-mail information alerts, represent important parts of the Internet exploitation. Yet this represents only about 30% of the total open sources. Moreover, unlike printed publications, anyone can post anything on the Internet—which increases the probability of obtaining fictitious or erroneous information if one relies on the Internet exclusively. This is commonly known as the "garbage in, garbage out" effect. Information relevance and correctness has certainly become an extremely sensitive issue. Furthermore, extant active Web agents called "intelligent agents," "network robots" or simply "bots" searching the Internet for specific information cover only about 15% of the visible Web, overlooking complex sites with many subsequent levels known as the "deep Web." On the other hand, bots can inundate one with vast quantities of data in response to simple queries. So Internet search engines might return thousands of links for certain queries while important information may be omitted if the usual keywords are missing. This degrades the practicability and usefulness of bots in some cases. Clearly, one must approach the Internet as just one of the open sources and be aware of its strengths and weaknesses. The Internet, despite its rapid growth, is more of a vehicle for open cooperation and collaboration than a reservoir of flawless and reliable knowledge.

Advantages and Disadvantages: The major advantage of OSINT is its accessibility. It is readily obtainable although it requires collection. Open sources are available extensively and that also makes OSINT less susceptible to manipulation and deception. Moreover, unlike covert operations, OSINT is not hazardous for the collectors. Furthermore, unlike any other intelligence category, OSINT products can be shared with virtually anybody, without requesting security clearances.

All of this makes OSINT extremely valuable for cooperation with civilian coalition partners and for intelligence dissemination in the multi-national non-Article-V operations.[6] As the role of the military shifts from collective defense to collective security, many non-traditional non-military cases require intelligence sharing with non-governmental and humanitarian organizations. OSINT appears to be a primary platform for such challenges.

In the case of NATO multi-national coalition operations, the involved nations tend to protect their national intelligence resources and their intelligence services do not cooperate well with each other. Yet, the same nations will be willing to use an open-source environment for both information gathering and intelligence sharing. So, in such a case, the combined joint command should initially use the OSINT process instead of turning to classified national intelligence collection. Moreover, NATO has usually no tasking authority over national intelligence assets while it can use open networks to propagate its intelligence needs without severe limitations.

The main disadvantage of OSINT is its abundance. Computer technology's ability to produce, to manipulate, and to store information increased exponentially, creating an information explosion. So, sifting through the information field to collect information that is relevant, correct, and needed has become more and more difficult. This is often called the "wheat and chaff" problem. As previously stated, single analysts and analyst cells cannot process all the available information. The intelligence community must find ways to create and to maintain virtual nets of information sources, OSINT collectors, and analysts.

Furthermore, military intelligence must use all the presently available options to disseminate OSINT products. Classified networks have the principal disadvantage for OSINT dissemination in that they must separate the products from the sources. Systems based on the Virtual Private Network (VPN) arrangement can provide ready access to the original materials with the advantages of security safeguards. The US system NIPRNET,

[6] Article V of the North Atlantic Treaty states that NATO members must consider coming to the aid of an ally under attack. However, it does not guarantee assistance. Article V is the Treaty's key provision. It states, in part, "…an armed attack against one or more allies shall be considered an attack against them all." Since the early 1990s, NATO has begun to adopt new missions, such as crisis management and peacekeeping, sometimes referred to as "non-Article V operations."

used by different US military services to share unclassified information, and the US Open-Source Information System (OSIS), which is a confederation of information systems serving the intelligence community with open-source intelligence, are examples of an OSINT sharing environment.

Naturally, OSINT is not an exclusive part of intelligence agencies—in practice, that is impossible. Open-source exploitation is relevant not only to the intelligence professionals, but also to all military personnel who may need open-source information. Indeed, intelligence professionals must support commanders and other decision-makers. But if adequate answers are readily available from open sources, engaging an intelligence agency is just pure inefficiency. Therefore, intelligence professionals should encourage their superiors and customers to manage their own open-source collections. If a robust OSINT system exists, it can save much time and reduce unnecessary requests for information. Once all staff elements have direct access to open sources, the intelligence staff can help facilitate the OSINT knowledge flow while evaluating sources and providing professional guidance.

All of the intelligence disciplines but OSINT have their dedicated collectors, processors and exploiters. In the case of OSINT, analysts are often expected to act as their own collectors. This situation would be considered preposterous if it happened in any other intelligence discipline. This flawed perception represents one of the major challenges OSINT faces.

Obviously, intelligence agencies under the pressure of cutbacks, reduction of personnel, and increasing intelligence requirements can hardly compete with CNN's worldwide coverage. So, military intelligence does not need to conceal its reliance on open sources or, even worse, to conceal that it collects open-source information by classifying it. Instead, it must develop its OSINT branch to be a state-of-the-art information collector and establish proper procedures to manage the vast amount of information that is available from open sources. Open sources should also be the first choice in the collection process because OSINT conserves resources by reducing the unnecessary use of costly covert means. And finally, OSINT represents a usable platform

for disseminating vast amounts of information and the unclassified finished intelligence products among national and international organizations.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CZECH MILITARY, INTELLIGENCE, AND OSINT

This chapter examines the status of the Czech military, intelligence services, and use of OSINT. The first section traces the current security environment of the Czech Republic focusing on the main security concerns of the state. Also, the principal tasks of the military are surveyed and categorized. The second section of this chapter introduces the Czech intelligence services, particularly, the military intelligence. Moreover, current intelligence requirements are listed as a base for further analysis of possible applications of OSINT. The last section follows the four stages of the knowledge system and process design to analyze OSINT in the Czech military intelligence.

A. CZECH SECURITY ENVIRONMENT AND THE MILITARY

The Czech Republic was established on January 1, 1993 and was grounded on the Czechoslovakian democratic tradition created before WWII. The Czech leadership had to consider the geopolitical definition and the external security environment that Czechoslovakia had faced since its creation in 1918. During this period, adverse powers militarily occupied the country twice—in 1939 and 1968. These interventions and the nation's subsequent loss of independence, accompanied with economic, cultural, and moral devastation weakened the nation's resolve to defend and nurture democratic values. This weakening even included the military defense of the state. These experiences also negatively distorted the public's image of the armed forces and the nation's international conduct.

1. New Security Environment

The Czech Republic, formerly Czechoslovakia, was a part of the Warsaw Pact for four decades. After the so-called Velvet Revolution in November 1989, the Czech Republic began developing a democracy. Dynamic changes in the political, economical, and social situation in Central and Eastern Europe during the 1990's, as well as increased globalization and international exchange, raised many national security questions. Now

being part of NATO, the Armed Forces of the Czech Republic have developed new defense concepts and doctrines as a result of such influences.

After removing the old communist regime in the 1990, the newly sovereign federation had to create a new security policy. Three years later, the Czech security had to be reconsidered again when the Czech Republic and Slovakia divided. From 1997 to 1999, the Czech security and military strategies had to be changed once again—this time moving away from a purely national posture toward a collective defense organization within the NATO structure.

Nowadays, although the Cold War is long over, the Czech Republic sees NATO as the key security organization in Europe. On 12 March 1999, the Czech Republic joined NATO, thus acquiring the security guarantees of a collective defense in accordance with Article 5 of the North Atlantic Treaty. NATO membership obligated the Czech Republic to reinforce its own defense capacity and to share in the defense of its allies. Participating in NATO involves assuming full responsibility for decisions and being prepared to share in their implementation. The new Strategic Concept, approved by the NATO summit in Washington in April 1999, expands NATO's fundamental tasks to include a share in crisis management throughout the Euro-Atlantic region, to develop a partnership and to cooperate with other states in the area.

Indeed, NATO is being transformed from an essentially military organization to a more political one. The likely accession of new member states from the Baltic in the fall of 2002 will further accelerate the metamorphosis of the Alliance from an instrument for delivering collective defense to an organization for managing collective security. The Alliance with less US military presence and with more involvement from its European members will certainly be different from the body "reinvented" in April 1999. Many European countries want to more actively ensure the security of the Euro-Asian region. The Czech Republic wants to assist actively in the important role played by the EU security bodies. The Czech political leadership sees a partnership in the Common European Security and Defense Policy (CESDP) as a way to further increase the responsibility and participation in the European collective security.

The current Czech defense policy is based on the hypothesis of the indivisibility of security and on the universality of basic human rights and freedoms. The Czech Republic is therefore by no means indifferent to the fate of other nations and regions. It identifies its own security with the global security situation and is prepared to work actively with the international community to solve these problems. The Czech Republic makes it a priority to solve crises peacefully, but it may decide to use force in accordance with constitutional law if necessary (NSS 2001).

2. Current Threats and Risks to Czech National Security

As already mentioned, the Czech Republic judges threats to its security in the wider Euro-Asian context. The international community is trying to maintain or to restore peace, to protect human rights and freedoms, to condemn and punish war crimes, to create democratic institutions, and to foster economic recovery and regional development. However, inconsistently applied political and economic reforms have generated a number of new problems, including lowered standards of living and booming organized crime and corruption.

The regions in the southeast and east of Central Europe pose the most serious global threats to European security and to Czech security in particular. The Balkan crisis has not been fully solved yet; religious and ethnic tensions have been rising in the Trans-Caucasus region and Central Asia; and a critical situation has also evolved in some regions of Russia. Economical and social instability in those areas, the spread of individual or group violence, and negative demographic trends are substantial, even though indirect, risks to Czech security.

Widespread political and economic migration results from regional conflicts and differences in the standard of living. Migration is a sensitive issue in the European cultural and historical environment. Insularity of some population groups condemns immigrants to the margin of society where they can be lured into individual and organized crime. In turn, the native citizens reject further immigration.

The end of the Cold War substantially relaxed many tensions and significantly lowered the risk of worldwide confrontation. After the Iron Curtain fell, the national threats for states on both sides of the curtain changed radically both in positive and negative ways. Now, new threats are surfacing while some long-term problems persist. In the case of the Czech Republic, the National Security Strategy, first established in 1998 and amended in 2000, lists nine possible threats (listed below). Only two of them are directly linked with military threats or attacks. The other seven deal with economical, political, terrorist, and drug proliferation issues. The potential security threats and risks are defined in terms of their probability as follows (NSS 2001):

(1) *Natural Disasters, Industrial and Environmental Accidents, Emergence and Spreading of Epidemics*: These risks, permanently present and highly topical, can emerge within a few hours or days, and their nature and extent are difficult to predict.

(2) *Disturbance or Abuse of Standard International Economic Relations*: Disruptions of flows of strategic commodities and raw materials, as well as attacks on computer networks or threats to security of information databases, represent significant danger to the internal economic affairs of the Czech Republic.

(3) *Individual Acts of Terrorism and Organized Activities of International Crime of an Extraordinary Extent*: Attacks against citizens and economic, infrastructural, or administrative facilities may inflict severe casualties. Although the Czech Republic is not considered a potential terrorist target, it cannot disregard such threats.

(4) *Massive Waves of Migration*: The vast number of immigrants to the country could become violent, both inside and outside the state's borders.

(5) *Violence by Alien Powers*: Foreign countries may conduct violence against persons or property in the Czech Republic because the country has participated in international peace-support operations or humanitarian missions.

(6) *Threats to Essential Principles of Democracy and Civil Liberties in Other Countries*: Internal political violence and low intensity conflicts outside the Czech territory could seriously endanger international security.

(7) Extensive Subversive Actions: Adverse forces can execute subversive actions to render the Czech Republic's defense assets useless and to disrupt the country's transition to the state of war.

(8) Direct Threat of Aggression. An attack against an allied nation is a direct threat to the Czech Republic.

(9) Direct Military Attack against the Czech Republic.

The risks listed in paragraphs two to six above are highly relevant. They can be initiated in combinations and can therefore produce threats that are difficult to predict. Such risks can be activated in a few days to several years. The military will only assist in eliminating such risks and its deployment will involve a limited use of combat assets.

The risks specified in paragraphs seven to nine above obviously pertain to the military. Their current probability is low, and they are easier to predict. Such risks can be activated in months to years, and they would inflict major destruction. To eliminate such risks, the Armed Forces would be engaged in progressively escalating combat.

3. Czech Military

The Czech military has marched along a crooked and rough road—from the highly politicized and anti-Western service of the 1980's to the NATO-allied army at the end of the twentieth century. Today, the Army of the Czech Republic (ACR)[7] is certainly different from that of twelve years ago. The early 1990's realigned the structure, the personnel, and the orientation of the Armed Forces owing to the end of the Cold War and the fall of the communist regime. The disinterest of top policy-makers in security and defense matters in the mid-1990's negatively imprinted the Czech military, leaving it

[7] The name "Army" does not have the same meaning in the Czech Republic as it does in the USA, for example. In the Czech Republic the word encompasses all three military services—the Ground Forces, the Air Force, and the Territorial Defense Forces. See the organizational structure of the ACR, described later in this chapter.

without any nation-level defense policy and allowing unsystematic decisions. And NATO membership brought a large set of new requirements during the late 1990's.

Indeed, the Czech military's doctrines, structure, and tasks have changed significantly since 1990. During the 1990's, the Czech Republic suffered drastic declines in the size of the military structure and personnel. Also, the cutbacks in the military budgets significantly eroded the combat capabilities, simply because the extent of equipment and personnel reduction did not match the decreases in funding. Moreover, until the succession to NATO, the Czech political leadership paid only limited attention to security and defense issues, which worsened some of the problems. Unfavorable public opinion, limited expertise of the top military leadership, controversial decisions about procurements and modernization, as well as shortages in the readiness and training accompanied the Czech Republic's integration into NATO.

Despite the Czech Republic's small size, the contribution to NATO's missions, although severely limited militarily, has become highly valuable politically. Recent participation in many UN-based or NATO-based operations, such as in the Persian Gulf or in the former Yugoslavia, has proved that the Czech Republic desires a useful role in alliance operations. As to the current comparisons with other countries of similar size and military capabilities, such as Portugal, the Czech Republic is not perceived as a "free rider" but rather is seen as an average or a below-average NATO member in terms of contribution.

Like other NATO members, the Armed Forces of the Czech Republic have earmarked most of their forces for the Alliance—78%. However, having all the units achieve the NATO standard capabilities, as set in the Force Goals is proving difficult. Given the current state of build-up, training, and logistic support of the forces, even high-priority units would have difficulties in terms of the required readiness, level of training, compatibility of weapons and equipment, command and control systems, transportability and mobility, firepower, efficient engagement, and force sustainability, if they were evaluated in accordance with the *Force Standards for the Rapid and Immediate Reaction*

Forces.[8] NATO standards and the interoperability requirements certainly represent the main NATO-related concern of the ACR. (ARCTSC 2001)

Now, let's focus on the principal tasks, the organizational structure, and the reform of the ACR. This will encompass the current and the future environments of the Czech military, thus providing a sufficient base for the knowledge system and process design.

Tasks: According to the National Military Strategy (NMS 1999), the ACR has four principal tasks:

(1) *To Defend the Czech Republic against an Outside Attack*: To defend the country's territory once an outside adversary has attacked it, the ACR will conduct operations either independently or together with NATO forces. The Armed Forces will assign and prepare one to two tactical groupings of peacetime strength units for rapid deployment to eliminate local destructive operations of forces organized along military or paramilitary lines. In the case of an extensive threat to national security, the ACR will continue to reinforce peacetime strength units as necessary. Also, it will prepare territorial defense elements to protect important facilities and assets in cooperation with other regular forces. To be able to defend its country, the ACR continuously prepares a build-up of troops to wartime strength and their deployment in a mobile, flexible, deep operational formation in order to conduct operations along one threatened axis, either independently or together with the allied forces. Moreover, the ACR builds and prepares the infrastructure to support operations of their own troops and to allow Alliance forces to be received and deployed in the country's territory. And finally, the Czech military provides for and conducts training of the professionals, conscripts, and reservists and participates in the education and training of Czech citizens for the defense.

[8] These standards have been established by the Allied Command in Europe (ACE) for the force performance evaluations at the tactical and operational levels (TACEVAL, or OPEVAL, respectively).

(2) *To Take Part in Defending the Alliance*: The Czech Republic, as a full member of NATO, partakes in protecting freedom, security, and other vital interests of all the Alliance members. To fulfill its obligations in accordance with the North-Atlantic Treaty, the Czech Republic established its NATO-command forces, NATO-assigned forces, and NATO-earmarked forces. These forces are built and trained as professional combined-arms formations and units, which are ready for airlift by allied air assets and can conduct operations outside the Czech territory as a part of the NATO task forces. As its top priority, the ACR develops and provides for compatibility and interoperability with the armed forces of the Alliance, paying particular attention to command and control systems, information and intelligence systems, and technical surveillance systems.

(3) *To Participate in Peace-Support Operations, Rescue-and-Relief Operations, and Humanitarian Operations*: The ACR takes an active part in peace-support operations and also participates in rescue, relief, and humanitarian operations abroad. It assigns forces up to a mechanized battalion plus a special company, the combined number of which is up to 1,000 people. The ACR builds and prepares military rescue units and other available peacetime forces capable of saving civilian population from dangers threatening their lives, health, or property. Depending on the tasks at hand, the military selectively reinforces and deploys specialized units to provide assistance in the event of a natural disaster or industrial accidents abroad.

(4) *To Participate in the Elimination of Non-military Threats*: The military can confront non-military threats to national security and can protect internal security and maintain public order within the country. To be able to participate in such tasks, the ACR selectively prepares a part of the ground, air, and territorial defense forces to act as reinforcements of the Police of the Czech Republic (PCR).

Organization: The current organizational structure of the Army of the Czech Republic is depicted in *Figure 4*.[9]

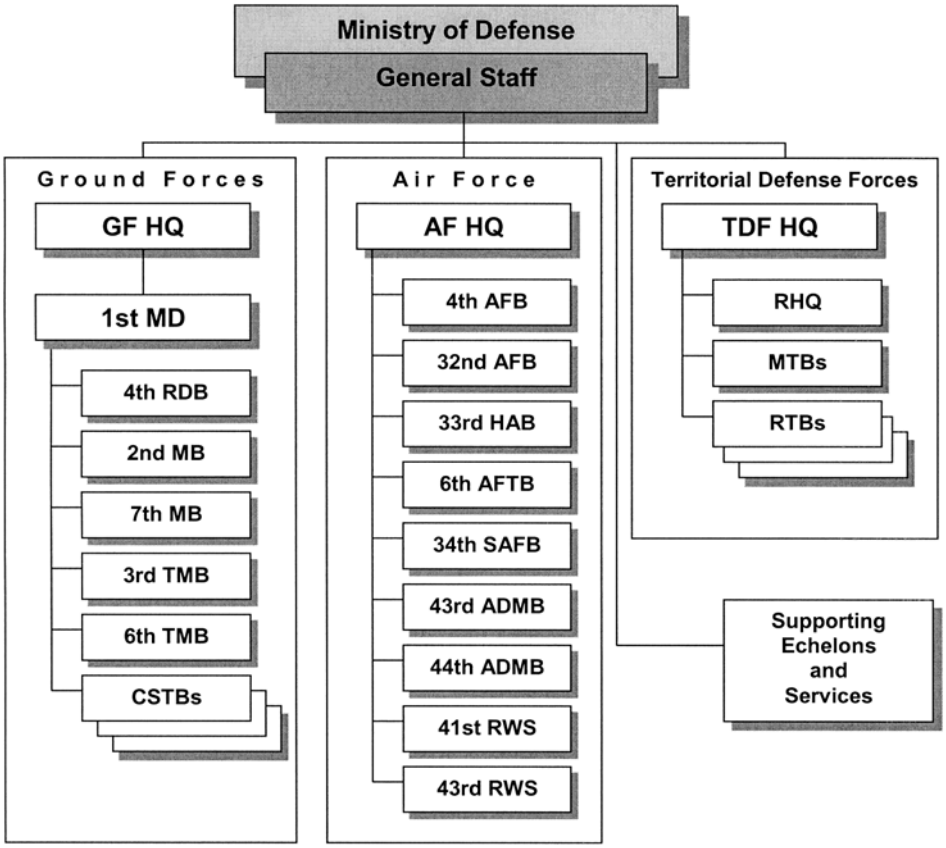


Figure 4. Organizational Structure of the ACR

[9] The figure depicts only main combat and support formations down to the brigade/base level. Legend: HQ = Headquarters; MD = Mechanized Division; RDB = Rapid Deployment Brigade; MB = Mechanized Brigade; TMB = Training and Mobilization Base; CSTBs = Combat Support Training Bases (one per each combat support element, i.e. reconnaissance and electronic warfare, signal, artillery, engineer, and chemical XXX); AFB = Air Force Base; HAB = Helicopter Air Base; AFTB = Air Force Transportation Base; SAFB = Special Air Force Base; ADMB = Anti-Defense Missile Brigade; RWS = Surveillance and Warning Sector; RHQ = Regional Headquarters; MTBs = Mobilization and Training Bases; RTBs = Rescue and Training Bases.

Reform of the military: The Czech military still has to overcome many negative preconceptions. Although some of the biases stem from the traditional Czech anti-military proclivities, low regard for the military should not be treated as something deterministic. Second, other more realistic problems, such as insufficient and ineffective planning and budgeting, lack of modern weaponry, incompatible command and communication systems, and unsuited proportion of personnel still exist.

The ACR has been continuously restructuring since its official formation in 1993. During the process, the ACR has attempted to adapt internally to the external environment. Much progress has been made, especially in preparing for membership in and accession to the Alliance. The invitation to the Czech Republic to join NATO and the fulfillment of the minimum military requirements as of the accession day is undoubtedly a great success. Yet, none of the restructuring processes undertaken so far has brought about a qualitative change in the ACR's capabilities. Also, many disputable decisions have been based upon political and personal interests, not always in line with the worldwide military trends. The purchase of the L-159 light attack aircraft and upgrading of the T-72 main battle tank, for example, have consumed substantial funds from the defense budget. (ARCTSC 2001)

The last reform of the ACR, started in August 2001, is designed to improve the position of the ACR in a democratic society and to allow the ACR to cope better with the present security risks and challenges while using the allocated funds most efficiently. The new military leadership, especially the Minister of Defense Jaroslav Tvrdík, clearly expressed the needs for more transparent management, high economic efficiency, and increased force effectiveness. For the ACR to fulfill the vital and strategic interests of the Czech Republic adequately, it must also have the required capabilities. Along with other alterations, reforming the Armed Forces will cause the following changes (Reform 2001):

- The Czech Republic will gradually shift to fully professional armed forces and cancel the conscript service. By 2003, the ACR will prepare the groundwork for necessary legislative changes toward all-voluntary forces; by 2005, all NATO-earmarked forces should be fully professionalized; by 2007, the Armed Forces will be all-volunteer personnel.

- The ACR will be divided into *Deployable Forces* and *In-Place Forces*. Furthermore, they will be sub-divided into *High Readiness Forces*, *Forces of Lower Readiness*, and *Long-Term Build-Up Forces*.
- Well-equipped, well-trained, and well-supported deployable forces will be the priority.
- The ACR will focus on developing passive surveillance systems and protection against weapons of mass destruction (WMD), particularly detecting and identifying chemical and biological substances.
- The ACR will improve its capabilities in psychological operations, deceptive operations and civil-military cooperation (CIMIC).
- By 2007, the Armed Forces will not exceed 34,000 to 36,000 active soldiers plus up to 10,000 civilian employees.[10] The maximum wartime numbers will not exceed 1.8 times their peacetime counterparts. [11]

The ACR's definite role remains the same—to guarantee the defense of the Czech Republic. Possible military involvement has these three alternatives:

- All Czech Republic's armed forces will participate in one major Article-V operation;
- The Czech Republic will send a brigade-size contingent (up to 5,000 persons without replacement) to participate in one operation for up to six months;
- The Czech Republic will participate in one long-term operation with a battalion-size contingent (up to 1,000 persons without replacement) and, concurrently, in another operation with a smaller contingent (up to 250 persons).

Aside from that, the ACR must be able to provide forces and assets for the Czech integrated rescue-and-relieve system inside the country.

[10] As of January 1, 2001, the Armed Forces totaled 69,296 persons; 23,184 of them were professional soldiers, 24,955 conscripts, and 21,157 civilian employees. See for example http://www.army.cz/reforma/english/docs/p07.htm.

[11] To better understand the insufficiencies of the ACR, as well as to apprehend the amount of work accomplished so far, one should see the analyses provided by the *Center for Preparation of the Armed Forces Reform*, posted at http://www.army.cz/reforma/index.htm.

Figure 5 illustrates the future organizational structure, as proposed by the conception.[12]

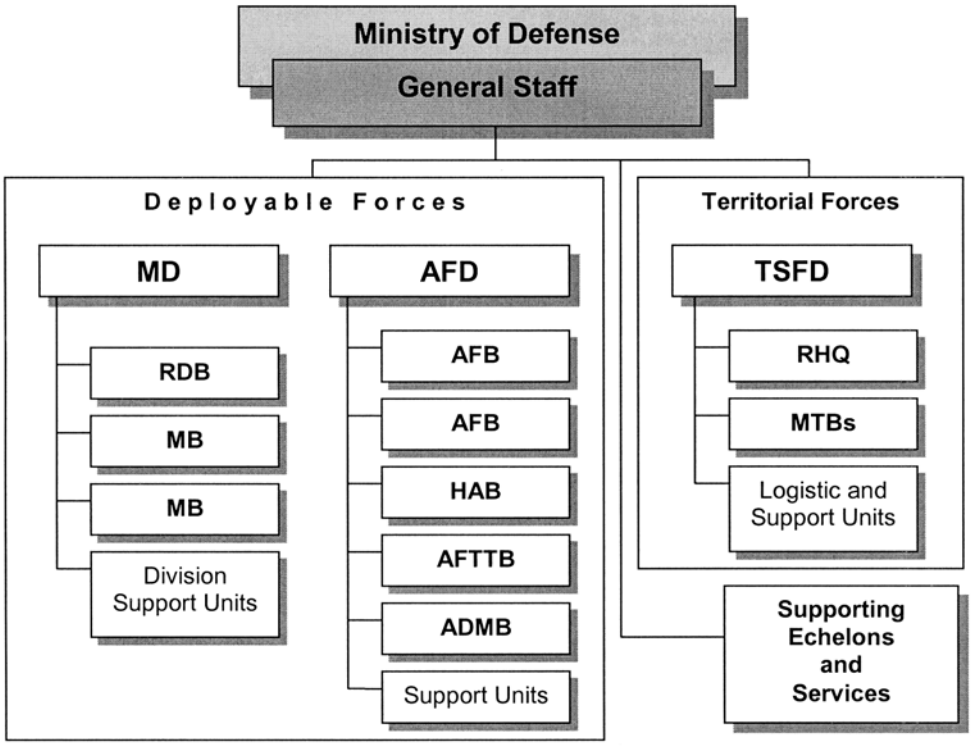


Figure 5. Organizational Structure of the ACR by 2007

Regarding the military intelligence, the reform concept stresses the importance of analytical outputs for the defense planning and preparation. Yet, the military intelligence will probably be included in the whole reformative package covering all Czech intelligence and counter-intelligence services. The intention to reduce the overall number of services has existed since the early 1990's, accompanied by various inter-agency "turf wars;" so it is likely that the military intelligence will face some reform in the near future.

[12] The figure depicts only main combat formations down to the brigade/base level. Legend: HQ = Headquarters; RDB = Rapid Deployment Brigade; MB = Mechanized Brigade; AFB = Air Force Base; HAB = Helicopter Air Base; AFTTB = Air Force Transportation and Training Base; ADMB = Anti-Defense Missile Brigade; RHQ = Regional Headquarters; MTB = Mobilization and Training Base.

As of April 2002, the *Conception of the Professional Build-up of the ACR* has been prepared and submitted for approval. The government acquainted with the document; however, with the upcoming elections in June 2002, the administration postponed the document's approval, leaving further reform-related decisions to its successor.

B. CZECH INTELLIGENCE AND COUNTER-INTELLIGENCE SERVICES

"I don't need intelligence services. CNN is enough for me." This comment, credited to Prime Minister Václav Klaus in 1994 (Hořejší 1997), summarizes the general attitude of both politicians and the public. This attitude has not changed much since 1990. The Czech intelligence services, including the military intelligence, underwent many reorganizations and management changes. During the mid-1990's the power over the intelligence agencies shifted from the President and Parliament to the government and Prime Minister, but they had little interest in exercising it. Only in the late 1990's did the government and the Parliament formulate basic policies, amend obsolete laws and create new ones, and constitute clearer oversight over the intelligence services.

After the split with Slovakia and the end of the federation in the 1993, the Czech Republic established four intelligence agencies, based on their federative predecessors:

- The *Bureau for Foreign Contacts and Information* (Úřad pro zahraniční styky a informace–ÚZSI), a civilian agency responsible for foreign intelligence;
- The *Security Information Service* (Bezpečnostní informační služba–BIS), a civilian counter-intelligence agency;
- The *Military Defensive Intelligence* (Vojenské obranné zpravodajství–VOZ), a military counter-intelligence agency;
- The *Military Intelligence Service* (Vojenská zpravodajská služba–VZS), the intelligence agency of the ACR.

Organization structures and tasks of the above listed services have changed slightly since then. Their core responsibilities are summarized in the following section.

1. Services, Tasks, Cooperation, and Oversight

The organizations and tasks of the Czech intelligence and counter-intelligence services are somewhat different from those in the USA, for example. Yet, the basic functions remain similar throughout the world—what usually differs is the actual numbers, subordination, flow of information, and oversight. In order to provide for a broader frame into which to fit OSINT later on, one should first understand the organization and main tasks of the Czech intelligence and counter-intelligence services.

Military Intelligence (VZ): In 1994 the Military Defense Intelligence (VOZ) and the Military Intelligence Service (VZS) were formally amalgamated into the *Military Intelligence* (Vojenské zpravodajství–VZ) through Law No. 153, or "intelligence bill" (ZZS 1994). But the two segments of the VZ practically work independently, even though a certain level of cooperation has been attained. While the former reports directly to the Minister of Defense, the latter is subordinated to the Chief of the General Staff. The subordination is illustrated in *Figure 6*.

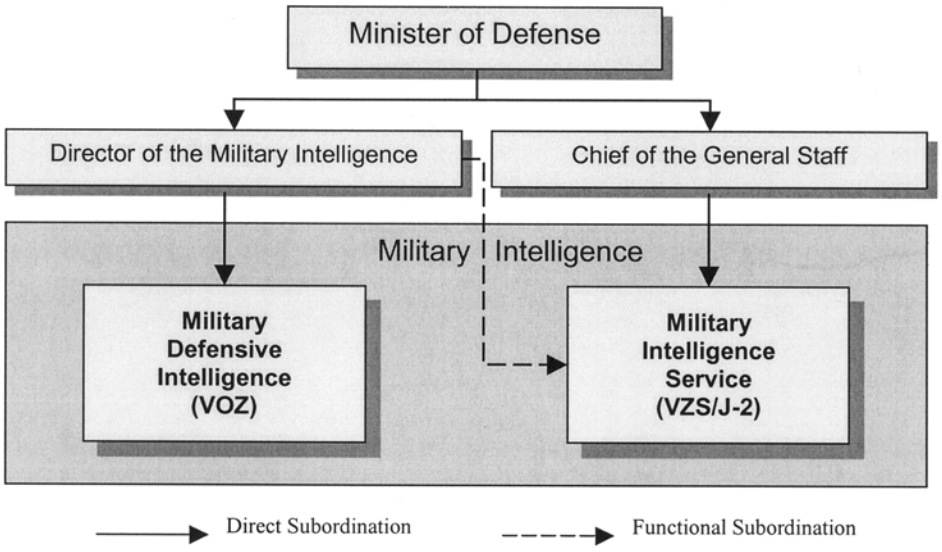


Figure 6. Subordination of the Military Intelligence Services

In accordance with law, "the Military Intelligence (VZ) provides the following information:

(1) Information about intentions and activities that represent military threats to the Czech Republic.
(2) Information about foreign military intelligence services.
(3) Information about intentions and activities directed against the assurance of the defense of the Czech Republic.
(4) Information about activities endangering state and service secrets related to the defense of the Czech Republic." (ZZS 1994)

The VZS has full responsibility for the first item in the above list. The other three items are mainly under the jurisdiction of the VOZ; however, the VZS participates in those tasks when gaining relevant information abroad. Moreover, the VZS not only fulfills the tasks of the military intelligence but also functions as the J-2 branch, being responsible for the military reconnaissance and electronic warfare at the strategic level.

Security Information Service (BIS): The Security Information Service (BIS) has probably been the most "torn and twisted" service since it represents a domestic intelligence bureau. As such, considering the very negative reputation the former totalitarian state secret police (State Security, or StB) earned, the BIS leadership has been under severe pressure from both the politicians and the public. Notwithstanding accusations of being politicized, the BIS is also known for numerous cases of misconduct among its members. Yet, one should be aware that the BIS lacks sufficient human and material resources while having to tackle a wide variety of tasks.

According to law, the BIS provides information:

- About intentions and activities, such as political extremism and subversive actions, aimed against the democratic institutions, sovereignty, and territorial integrity of the Czech Republic;
- About foreign intelligence services;
- About activities compromising state and service secrets;

- About activities endangering the security or important economic interests of the Czech Republic, such as corruption, money laundering, WMD and arms proliferation, and so on;
- About organized crime and terrorism.

Although successful and publicly praised in some cases, the BIS is often cited for its insufficient coverage of foreign espionage and organized crime. An enormous turnover in personnel is probably the most serious cause of such problems.

Bureau for Foreign Contacts and Information (ÚZSI): According to its vague mandate, the Bureau for Foreign Contacts and Information (ÚZSI) provides for "information originating abroad important for the security and protection of the foreign-policy and economic interests of the Czech Republic." (ZZS 1994) The ÚZSI studies global risks, such as terrorism, extremism, proliferation, drugs and arms dealing. The activities of the ÚZSI and its intelligence productivity remain close to the public. Yet, it is known that, owing to the shutdown of espionage after 1989, the ÚZSI has continued to work largely from open sources and via liaison officers abroad.

Interagency Cooperation: Cooperation among the services is based upon inter-agency agreements that the government must approve. Moreover, each agency can exchange information with its foreign counterparts and other services if approved by the government. Statistics, related to the amount of cooperation among different services, if any exist at all, are not publicized. Probably the largest amount of information is exchanged between the BIS and the police, owing to the fact that both services cooperate closely in combating corruption, organized crime, and terrorism. As for the Military Intelligence (VZ), its two parts, the VZS and the VOZ, have connected with tens of intelligence and security agencies and also integrated into the intelligence system of the NATO Allied Command in Europe (ACE).

Direction, Reporting, and Oversight: The President and the government task intelligence services in accordance to their respective functional areas. The Czech government coordinates all the services via its permanent *Intelligence Committee* and

bears the responsibility for the services' activities. Practically, all the services except for the BIS are subordinated to a ministry. The director of the ÚZSI reports to the Minister of Interior and the director of the VZ is subordinated to the Minister of Defense. The director of the BIS, however, answers to the entire government. The subordination of the ÚZSI and BIS are not what one would normally expect but rather a result of the mistrust of domestic intelligence.

All the services prepare and submit their annual reports to the President, the government, and their respective ministers.

As to the parliamentary oversight, the Parliament exercises direct oversight only over the two counter-intelligence agencies—BIS and VOZ. However, the Intelligence Committee advises the Parliament of the activities of all the intelligence services on a regular basis.

2. Current Military Intelligence Requirements

Since the Czech Republic gained its independence, both politicians and the public have perceived the defense planning and especially the role of military intelligence as entirely theoretical. Unlike Poland or Hungary, where instability in the former USSR states or the Balkan crisis continues to shape the states' defense policies, the geographical location of the Czech Republic, its succession to NATO, and the absence of a direct threat make the country highly unlikely to be threatened militarily. The hypothetical threats from Germany and Russia would endanger the Czech Republic's sovereignty, but such threats are very unlikely to occur. More likely, the Czech Republic can be involved in regional, border, or internal conflicts that will not affect the country so radically. Fortunately, the Czech Republic security establishment sees the NATO and European security and economic institutions as sufficient tools to deal with such conflicts effectively. Finally, a conflict with Slovakia also seems to be extremely unlikely, for no serious border or minority problems have occurred since the split in 1993.

Although the probability of a direct military attack against the Czech Republic has been significantly reduced and is unlikely in the near future, military attacks cannot be

ruled out completely. Indeed, the most probable threats in the foreseeable future are organized crime, terrorism, and waves of refugees; such problems may cause internal instability and unrest. Especially terrorism or international crime may infiltrate the Czech Republic—and being endangered by a force of such a magnitude the country may need the military to eliminate the threat.

In practice, the shift to non-military and semi-military threats and risks has changed the intelligence requirements. The VZS, although still tasked to assess traditional military targets, is becoming more and more involved in providing intelligence about other non-military topics as well. The following briefly covers the areas that deserve the attention of the military intelligence.

Weapons of Mass Destruction: The threat of nuclear weapons and other weapons of mass destruction (WMD) has not been totally eliminated. The expanding group of entities with these weapons or attempting to acquire them is particularly disturbing. These entities are often states with non-democratic and unstable regimes. It is especially dangerous when individuals or non-state entities control weapons of mass destruction, whatever the quantity, however few. Intelligence predicts a significant risk of such an encounter within the next few years.

Traditional actors may also pose significant danger to the global security. The chance of war between India and Pakistan is now greater then ever in the last three decades. Although both states are publicly downgrading the risk of nuclear conflict, a conventional war could escalate into a nuclear confrontation. Iraq's regime continues to restore its military force and to fund its pursuit of WMD, despite its own positive diplomatic efforts toward the UN and neighboring states. Furthermore, NATO states can face threats from the inter-continental ballistic missiles (ICBM) that exist or that are being developed in North Korea, Iran and Iraq.

When developing advanced weapons, WMD proliferators build upon the experience of others and take advantage of the dual-use nature of WMD-related technologies. For example, networks of fictive companies and organizations help conceal the transfer of radioactive materials, coming to the Czech Republic mostly from the former Soviet Union. Many chemical and biological weapon (CBW) facilities are hidden

in plants that are very hard to distinguish from genuine commercial sites. Unlike nuclear or chemical weapons, bacteriological weapons can be constructed in very small laboratories within a few days. That is why all WMD transfers, including delivery means, special components, and production technology are one of the main concerns of the intelligence services in all democratic countries.

Terrorism: Count de Marenches, former head of the French intelligence services, insisted that the Cold War was really World War III, and that World War IV is now under way, full of new enemies. He predicted in 1992: "The Fourth World War will be a terrorist war." (Marenches and Andelman 1992) Unfortunately, he seems to be right and the recent tragic events of September 11, 2001 have confirmed his prediction.

Domestic unrest and political, religious, or ethnic conflicts in weak states are factors conductive to terrorism. The problems terrorists exploit—poverty, alienation, and ethnic tensions—are estimated to increase over this decade. The world's poorest and most politically unstable regions in Asia and Africa will have the largest youth population in the near future, expanding the recruiting potential for extremist groups.

Intelligence services generally fear that not only conventional explosives but also nuclear, chemical, or biological weapons could be used as a means of blackmailing the government or international organizations. Terrorist groups have ready access to information on WMD via open sources, especially the Internet.

So far, the Czech Republic has not been a terrorist target. Although over two hundred explosions have been recorded since 1990, all the cases were labeled as the work of amateurs without detectable political motives. Yet, adversarial groups or individuals may use the Czech Republic as a base for attacks in other states, or they can attack Czech-based institutions, such as embassies or the Radio Free Europe/Radio Liberty in Prague. In general, terrorists can target high-profile government facilities, famous landmarks, and infrastructure nodes, such as airports, bridges, and dams. To stop or prevent such attacks is enormously difficult, and the intelligence services play an exclusive role when collecting and analyzing information on the intentions and movements of terrorist groups and individuals.

In a number of regions, Islamic fundamental terrorism in particular is already a frequent and dangerous phenomenon. The region closest to the Czech Republic that is important to the military intelligence is the Balkan Peninsula. Furthermore, worldwide organizations, such as Al-Qa'ida, Hamas, Hizballah, and others that have already planned and successfully accomplished various strikes against allied targets in Europe and must be monitored attentively.

Information Warfare:[13] High performance electronic information systems have created global network cyberspace. Not only were corporate businesses and governments able to attain high technology, but also tens of millions of individuals suddenly within less than a decade gained tools and capabilities, which had been previously limited to a selected few. Today, many state and local governmental organizations are establishing a presence on the Internet. Also, thousands of private agencies are reachable via online information services. That has radically complicated what intelligence agencies had to face in the past into something very complex now, and which will be even more troublesome in the future.

The Czech military often depends on civilian information networks. Most of the peacetime military communications, for example, travel over the same phone networks used to fax a contract or to talk with a friend. Also, the national electric power grid powers military and police bases. Purchases for military organizations are paid via the commercial banking network. People from national security organizations are transported under the guidance of civilian rail and air traffic control systems. Each of these information or transportation nodes creates a substantial vulnerability for the military in a crisis.

Today, one who controls information controls people. Relying on information systems presents an attractive but two-sided opportunity—intelligence can use information systems effectively to gain, store, and retrieve information but adversaries can also attack such systems. Such development has created the *information war*. An

[13] Although some authors see information warfare (IW) more as a combat arm, it definitely represents a highly topical issue for the military intelligence. However, the extent of IW is so wide that it exceeds the scope of this thesis. To better understand IW and its relation to terrorism and organized crime, see the works of Arquilla, Denning, Ronfeldt, and Schwartau.

information war has no front line. The potential battlefields are anywhere networked systems allow access. Information warfare is a low-budget, high-tech vehicle for mass destruction. (Schwartau 1996) Indeed, cyber terrorists attack information networks relatively cheaply already.

Organized Crime: Offenses such as arms proliferation, smuggling, computer crime, drug trafficking and other crimes directly impact the Czech Republic citizens and economy, regardless of their origin. The democratic development and still primitive tools for maintaining security in the Czech Republic are attractive targets for criminal activities. Transnational organized crime is currently the greatest imperilment. The Czech Republic is attractive both as a market and a transit route due to the weaknesses in its legal, policing and judicial structures. The political, social, and economic changes occurring in Eastern Europe and in the former USSR have provided significant, unintended opportunities for organized crime and criminal enterprises. Illegal syndicates set up their underground networks for illegal migration, drug trafficking, and arms proliferation.

Criminal organizations operating in the Czech Republic come mainly from the countries of the former Soviet Union, former Yugoslavia, and Bulgaria, together with those from Italy and Southeast Asia. For example, Asian criminals, especially Vietnamese, have been involved in organizing illegal migration and smuggling goods. Arabian, Yugoslav and Albanian groups concentrate on drugs and deal in arms. Well-organized criminals from Russia, Ukraine, Chechnya, and the former Yugoslavia are becoming more aggressive and are typically involved in criminal violence. The groups from the former USSR are now the most active, merging with various illegal groups that operate internationally.

As to the illegal migration, refugees crossing Czech borders in recent years decreased because of improvements in Kosovo. Yet, the number of fugitives from other parts of Europe and Asia increased. Some foreigners do not legalize their residence in the Czech Republic and participate in various criminal activities. Their arrival and residence

is mostly planned and conducted by internationally organized groups.[14] Indeed, illegal migration is moving mostly from the East and Southeast to Germany. Statistical data confirm that the Czech Republic remains a transit country for fugitives on route to Western Europe (Zpráva 2000).

Narcotics and drug proliferation is another threat that spreads across borders. The narcotics have become a global problem that is likely to rise dramatically in the Czech Republic in the next few years. Statistics on illicit drug consumption in the Czech Republic[15] indicate that drug use and drug trafficking is on the rise. The Czech military has not participated in any particular anti-drug operation so far; however, the ACR should not exclude the possibility of being involved in a larger anti-narcotic operation.

Illegal trade in arms and explosives has remained almost constant recently. Criminal groups illegally sell and purchase explosives, weapons, and ammunition with no identification marks, frequently offered on the black market.

Economy: We traditionally tend to think in either military or economic terms, instead of recognizing the synergy of the two and treating them as a single concept. The collection strategies of adversaries and allies alike will not only focus on defense-related information but will also focus on scientific, technological, political, and economic information. Misinformation, blackmailing, destruction, or other means of economic disruption must be anticipated. From a military perspective, economic vulnerability of well-developed countries as well as the economy of potential adversaries should be

[14] In 2000, 32,720 persons were apprehended while illegally crossing the national borders; 94% of them—30,761 persons—were foreigners. Most were from Romania, Afghanistan, Moldavia, Sri Lanka, India, Ukraine, and Bulgaria (Zpráva 2000).

[15] Estimated numbers of consumers (based on the demand side) for the year 2000 were as follows:

- Marijuana and hashish: 250,000 consumers
- Pervitin (a Czech-made, ephedrine-based synthetic drug): 22,500 consumers
- Heroin: 15,000 consumers
- LSD: 6,540 consumers
- Ecstasy: 5,820 consumers.

Illicit drug consumption totaled 0.8% of the GDP. *Note*: According to researchers, the numbers are probably underestimated due to very insufficient data collection, particularly in the case of Ecstasy (SANANIM 2002) .

considered when providing intelligence to commanders and policymakers because economy plays a very important part in a country's development.

C. OSINT IN THE CZECH MILITARY INTELLIGENCE SERVICE

In the age of information, intelligence is less a matter of penetrating secrets, and more a matter of extracting useful information from the flood of open information that is legally and cheaply available. The single most significant step an intelligence organization can take to increase the value of the information it acquires is to increase the speed with which the information is acquired and acted upon (Steele 1993). Yet, this would not be enough. As explained in the previous chapter, information is just a middle part of the pyramid—even if information is timely and accurate, it has no value unless it is used to create, distribute and use knowledge in decision-making processes.

The Czech military intelligence must react to the enormous impact open sources and information systems have on all aspect of intelligence dealings. The VZS can differentiate itself not solely by what collection assets it has at its disposal or how much or how little money it spends, but rather on the basis of what its people know. The author believes that OSINT, built on the knowledge management principles is a useful concept that can meet the consumers' needs. Some older practitioners may consider the concept revolutionary—but it is actually rather an incremental step that should be taken to manage open sources properly, using the advantages of modern information technology.

Indeed, the thesis will not provide a full analysis and a complex solution for OSINT knowledge management in the military intelligence—this is not a task for one person and a few months of research. However, by focusing on the challenges that should be considered, the four stages of the knowledge system and process design used in this section will help explain the role of OSINT in the Czech military intelligence. The section identifies target knowledge that can be acquired via OSINT, analyzes current OSINT procedures, and also identifies processes that must be addressed in future OSINT development. The section targets the Military Intelligence Service (VZS) in particular;

however, when appropriate, generalizations are made to express the broader applicability of the knowledge system and process design.

1. Process Analysis

In this first stage of the knowledge system and process design, attention is paid to objectives and strategies of the ACR in order to identify the knowledge that OSINT can attain and the VZS can manage. The OSINT system must not be built without understanding the tasks of the VZS; for each process, the knowledge that can ensure an effective performance must be defined.

First of all, the VZS serves as a decision-making tool for the strategic military commander, namely the Chief of the General Staff. Although some daily practices may suggest otherwise, the VZS is an organization that must provide military related intelligence—its first and foremost role. This role implies that the VZS builds its knowledge base upon the objectives and strategies of the ACR.

The objectives and strategies of the ACR have already been introduced in the previous sections. Now, combining the potential security threats and risks with the principal tasks of the ACR, the use of the Armed Forces is summarized into two main categories, each of which comprises a subset of probable tasks:

a) *Inside the Territory of the Czech Republic*: The ACR can be employed in the case of a threat or a risk that may have a direct impact inside the Czech Republic. The ACR may be particularly engaged to counter:

- Acts of the international organized crime of larger extent, such as proliferation of arms or weapons of mass destruction (WMD), drug trafficking, and extended communication and computer network attacks;
- Terrorist activities, either intended or realized;
- Immigration waves of a large magnitude;
- Natural disasters or technological accidents.

b) *Outside the Territory of the Czech Republic*: The ACR can be involved in military and non-military activities to prevent or to counter possible threats that

may have both direct and indirect impact on Czech or European security. Most likely, Czech troops will not act outside their territory on their own but rather under the umbrella of the UN or NATO operations, or as a part of the CESDP rapid reaction forces. The ACR may be employed in:

- NATO operations, either under the Article 5 or in non-Article-5 operations;
- UN-lead peace-support operations;
- UN/EU humanitarian missions of various nature;
- Actions realized under bilateral and multilateral military cooperation, such as the Partnership for Peace (PfP) program, military exercises, on-demand expertise, and so on.

One can easily see that most of the above mentioned tasks are of a non-combat or semi-military nature, although the military engages its combat assets during those missions and the possibility of direct combat cannot be excluded. Operations may not necessarily be waged against single and easily recognizable foes.

The ACR will likely participate in the missions abroad more frequently than engage inside the country. Intelligence needs for such missions seem to be relatively straightforward, considering the contemporary dynamic mode of operations. At the strategic level, there will generally be less need to discover the intention of an aggression, as in such cases the adverse activities will already be occurring. But the VZS will certainly need to gain and to use knowledge related to the local political situation, culture, demographics, terrain, weather, infrastructure, and composition and deployment of hostile and friendly forces. In some cases, such as WMD industry issues or technological disasters, very specific knowledge and expertise may be required.

U.S Ambassador Kimmit's requirement of the intelligence "an inch deep and a mile wide, with the ability to go a mile deep on any given issue" is certainly valid for the VZS as well. Yet, there is probably no intelligence organization in the world that is able to manage such a requirement solely on its own. That applies to the VZS in particular, knowing the limitations and circumstances under which the organization operates.

2. Knowledge Analysis

This second stage of the knowledge system and process design results from the previous analysis. In this part, the analysis concentrates on identifying the knowledge that is needed within the VZS.

When asked, the top VZS management confirmed that the service is now more involved in non-military topics than in traditional military subjects. As foreshadowed in the second chapter, the VZS simply cannot use only its own secret collection and analytical assets to cover the customers' needs—and neither can it acquire the required knowledge through OSINT itself. In all issues, OSINT must function as the first instance, as a broad knowledge base and as a knowledge gap filler.

Let's now have a brief look at the knowledge that can be build via OSINT and what purpose it may serve.

Warning: Military commanders and defense policy-makers will always be concerned about strategic warning. OSINT can provide a sufficient base for monitoring events that can potentially endanger the nation's existence, focusing on three main issues—nuclear attack, conventional attack, and unconventional developments.

As already mentioned, the nature of nuclear attack has changed. Arms reduction and the close monitoring of traditional nuclear powers, such as Russia or Kazakhstan, have been effective. On the other hand, the growing list of other nuclear-capable states consists of many unstable regimes whose interests and policies are contentious to those of the Czech Republic and its allies.

Conventional attack warning will probably remain an everlasting concern for the military intelligence, maybe even more so when the nuclear threat has diminished. Possible forward force deployments and military engagements in crisis regions is the reason for a continuous "intelligence watch."

Insurgencies, terrorist incidents, humanitarian crisis, and so on represent unconventional developments. The ACR and its allies will likely be encountering such developments more frequently. The Balkan situation, for example, represents an area of uncertain Czech policy interests but definitely continues to have the potential for

humanitarian crisis or other disasters. Instability in Central Asia threatens gradually to involve many regional powers, such as Russia, Turkey, China, Iran, India, and Pakistan. These developments, however, can be sufficiently monitored using open source news alerts and similar expert services. Also, non-state actors that use terrorism as "cheap warfare" frequently come from revolutionary, sectarian, and extremist religious groups, knowledge of which can frequently be through OSINT. Similarly, the VZS will mostly turn to open sources when seeking for knowledge related to international crime.

Peace Keeping/Peace Enforcement Operations (PKO/PEO): Kuwait, former Yugoslavia, Afghanistan—what will be next? For many years, Czech military units and individuals participated in peacekeeping operations; yet the military intelligence supporting those in the peacekeeping missions remains far from ideal. The intelligence support must not be aimed only at the top political-military command, i.e. the Ministry of Defense and the General Staff, but also at the troops in the field. Indeed, as both the VZS and the military units gained experience with the PKO/PEO, the situation has improved since the Persian Gulf War. However, the national intelligence support to the troops in the field is not systematic yet. OSINT can provide far more than narrow secure intelligence channels because it has the advantage of unlimited distribution and sharing. The military intelligence elements detached to support the peacekeeping forces also need—besides the traditional intelligence on orders of battle or weapons and equipment—detailed information about ethnic and religious groups, belligerent leaders, political parties and factions, military and civilian infrastructure, social structure, humanitarian needs, and so on. Obviously, not only military intelligence personnel but also every soldier on the field has a part in OSINT for the PKO/PEO.

Technology Proliferation and Arms Control: The issue of technology proliferation relates to both military and non-military technology and has become very complex. Military proliferation includes WMD, conventional systems, as well as support systems, such as command-control-communication-computer-intelligence systems (C4I), and associated technologies. The Military Intelligence Service (VZS) will have to keep up with the expanding transnational flow of subject-related knowledge. Fortunately, much of

what is needed is available from the open academic and industrial sources; yet preserving and upgrading relevant knowledge will be very challenging, should the VZS continue to track the flow of technologies and knowledge. The interchangeability of technological application between military and commercial sectors and the transnational nature of technology proliferation further complicate this issue.

Other Transnational Issues: Natural disasters, population dislocations, epidemics, environmental pollution, and similar uncontrolled large-scale problems can exacerbate regional instability; so the military intelligence will be tasked to focus on such issues should it become the concern of political leaders and military commanders.

Large numbers of people have become displaced economically or as a result of ethnic and religious conflicts in the former Soviet republics, the Balkans, Eastern Europe, and other places. These people move to the political and economical refuges of Western Europe and North America where the receiving countries experience pressures in terms of social services, housing, and increased ethnic dissension. The Czech Republic is embroiled in this pressure as it frequently serves as a transit country.

Significant health problems result from mass starvation and epidemics of diseases such as AIDS. Also, older forms of diseases, such as tuberculosis are reemerging owing to the recent conflicts in the Balkans, Chechnya, and other places and to uncontrolled migration.

Environmental concerns, such as hazardous waste disposal and the safety of nuclear power plants have also become important, being exemplified by the Chernobyl disaster or by the gradual destruction of most of the drinking water supply in Russia.

Photographic intelligence assets or other parts of the military intelligence may be tasked to contribute when a nation tackles the above-listed problems. Indeed, if it were tasked to provide intelligence on these issues, the VZS could not manage required knowledge without a connection to the outside open-source world.

Central to this part of the knowledge system and process design is identifying and analyzing *critical success factors* (CSFs)—activities that must be performed effectively in order for the mission to succeed. The CSFs must be in harmony with the organization's

core competency, namely providing intelligence for military commanders and other intelligence customers. The VZS may need a detailed study of its own tasks and capabilities to identify what knowledge is crucial to assess performance in the VZS' organizational setting and context. After the study is conducted, each of the factors should be separately evaluated as a single-target process. Using pre-defined configuration measurements, an existing configuration must be diagnosed in terms of process pathologies to determine how well does the existing process meet the desired goal. The diagnosis then helps eliminate the pathologies from the process.

3. Context Analysis

In this phase of the knowledge system and process design, knowledge—particularly the tacit knowledge possessed by specialists—stemming from OSINT should be captured. Once captured, the VZS can use information systems and other software applications to organize, to formalize, and to distribute the knowledge.

Organizational knowledge starts with individuals. The VZ must first recognize the knowledge its members possess, capture it, share it throughout the organization, and reuse it. In this way, the members amplify the knowledge and internalize it as a part of the organization's knowledge base. The management must be aware that intellectual capital is the most valuable asset. Collection tools and modern IT can acquire, process, and share information—but the knowledge of employees, experts outside the VZ, and the consumers of intelligence is what must be fostered and leveraged most. Managing knowledge is much more than merely storing and manipulating data—managing knowledge also recognizes the human assets that can be accessed and used by those who make decisions.

Without understanding the nature and organization of knowledge, the military intelligence personnel can hardly be effective in OSINT. An intelligence analyst, for example, may be both the seeker and provider of open-source knowledge in some cases. When solving a problem, the analyst can reach a point when further knowledge is required. The same analyst then can identify, capture, and organize the knowledge

needed. In other situations, analysts will outsource this knowledge work when they lack the time, propensity, or ability to do it by themselves. Then, the analyst will just use knowledge delivered by the provider. And this example is valid virtually for all knowledge workers, whether they solve intelligence requirements or daily routine work.

The VZS should develop knowledge maps to identify who possesses what kind of knowledge, both inside and outside the organizational structure. In order to build a foundation of open-source knowledge, the VZS must create "yellow pages" and knowledge maps of military and civilian experts and analysts. To accomplish this, first the organization's internal documents, the Intranet, databases, and directories must be carefully studied to identify and capture the OSINT knowledge already existing inside the VZS. Then, virtual network organizations, research and development (R&D) centers, librarians, annual reports and conference proceedings, association directories, and many more sources can and should be mapped to create maps of knowledge existing outside the VZS' organizational structure and to identify how this knowledge can be reached.

This whole procedure will certainly take much effort and time. Yet, it is probably the only systematic way to identify existing open-source knowledge and capture it. It will also help to find if any overlaps or inefficiencies exist in the extant or generated OSINT system and process design.

4. Systems Analysis

In this final stage of the knowledge system and process design, the organization's current procedures and information systems are briefly analyzed. First, the organizational design is surveyed. Then, controlling strategies and the information-flow configurations are summarized. Finally, the analysis basically follows the six phases of the knowledge management life cycle (KMLC), describing each particular phase in terms of extant procedures and practices within the VZS. Personal conversation and a written questionnaire[16] were used to expand the author's personal experience with the VZS.

[16] The sample consisted of ten VZS employees. Five of them were analysts; the other five were supervisors.

More detailed process and systems analysis is certainly desired, should the future knowledge design for OSINT be developed. However, the following paragraphs convey basic ideas about the VZS' organization, procedures and practices.

Organizational Design: A contingency model (Jansen et al 2000) is used to determine the current organization type of the VZS. The model explains the reason a specific form of knowledge management may or may not work in the OSINT. Here, the model is used to identify the whole organization; however, it will be useful to apply it to multiple VZS levels.

The contingency model uses four general strategies for knowledge management that differ from one another as to complexity and variability of the organizational environment. The model and the position of the VZS are depicted in *Figure 7*.

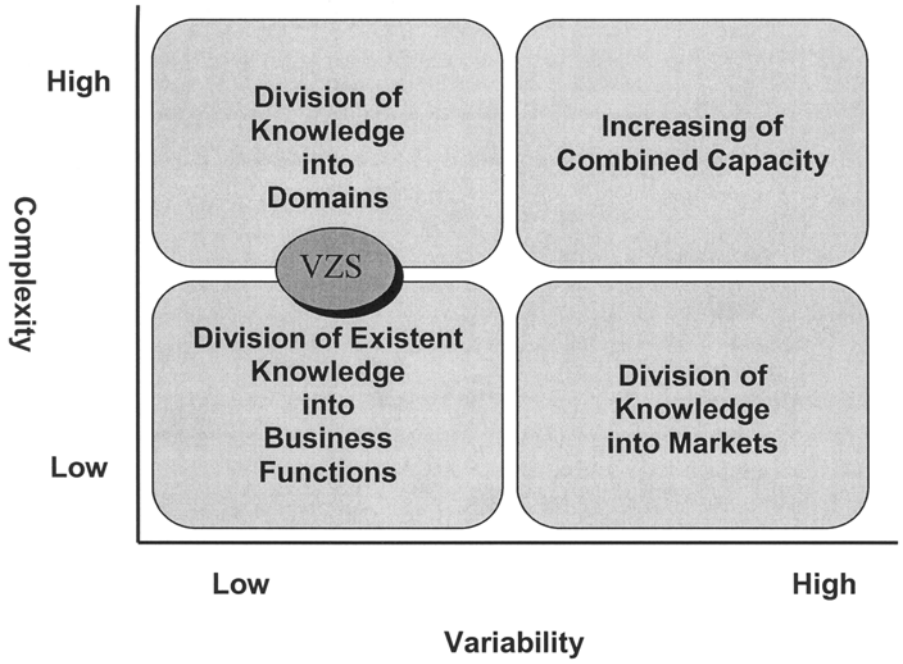


Figure 7. Four Strategies for Knowledge Management and the VZS

The current organizational design of the VZS and its information and communication technology does not exactly fit any of the four illustrated types. While the organization's structure evidently has some elements of the division into business functions, in some parts the VZS reveals existing domains of expertise. *Table 1* summarizes the main characteristics of the extant organizational design and IT.

Organizational Type	Organizational Design	IT and Communication
Division into Business Functions	• Centralization • Staff Organs • Rules and Procedures • Separate Departments	• Formal, Central Information System Focused on Compilation and Retrieval • Intranet
Division into Domains	• Separate Knowledge Domains • Individual Knowledge Levels • Group Knowledge Levels	• Generally Accessible Information System • Newsgroups and Bulletin Boards within Some of the Knowledge Domains

Table 1. Characteristics of the Extant Organizational Design and IT in the VZS

Dividing existent knowledge into business functions is mostly used in situations that are neither complex nor dynamic, and the organization does not actually create knowledge but frequently uses and refines it. Although this is not the case, the organization of the VZS is divided into separate functional departments and sections. The knowledge is also concentrated in the minds of individuals and very small, enclosed information entities. This is definitely a concept of the past when the required knowledge was clearly defined and this functional form was effective. However, this approach is still valid when existent knowledge must become explicit and when individuals want to use the knowledge.

Dividing knowledge into domains or areas of expertise is characteristic by dividing activities into different professional domains. Specialists for limited areas of expertise have the appropriate knowledge at their disposal; and the VZS management often uses these specialists to solve complex problems by creating ad hoc teams or cross-functional projects. The knowledge is used; the focus stays more on the application of implicit knowledge that the experts possess, rather than on knowledge content or knowledge creation.

It is no wonder that, in practice, the VZS has to adapt its organizational character and alter the strategy of knowledge work. The dynamics of information environment and variable requirements do not fit the military hierarchy well. Today, the adaptations are merely a passive reaction to the disordered outside environment. But the VZS should actively decide to choose a different path and should become an organization that creates knowledge, making it a more virtual, project-oriented enterprise. OSINT is the foremost arena where such a shift is possible.

Controlling Strategies and Information Flow: The existing organizational structure of the VZS, with its vertically oriented control, fully reflects the traditional military hierarchy. A simplified version of controlling and collaborating is illustrated in *Figure 8*. The structure of the VZS is formally built to let knowledge flow up while controlling its distribution down. However, the incoherent changes in the outer dynamic environment often force the organization's elements to collaborate in the horizontal directions, both formally and informally. The two functions of the VZS, i.e. the function of the defense intelligence agency and the function of the strategic directorate for reconnaissance and collection have created organizational difficulties, supporting stovepipes of the information flow.

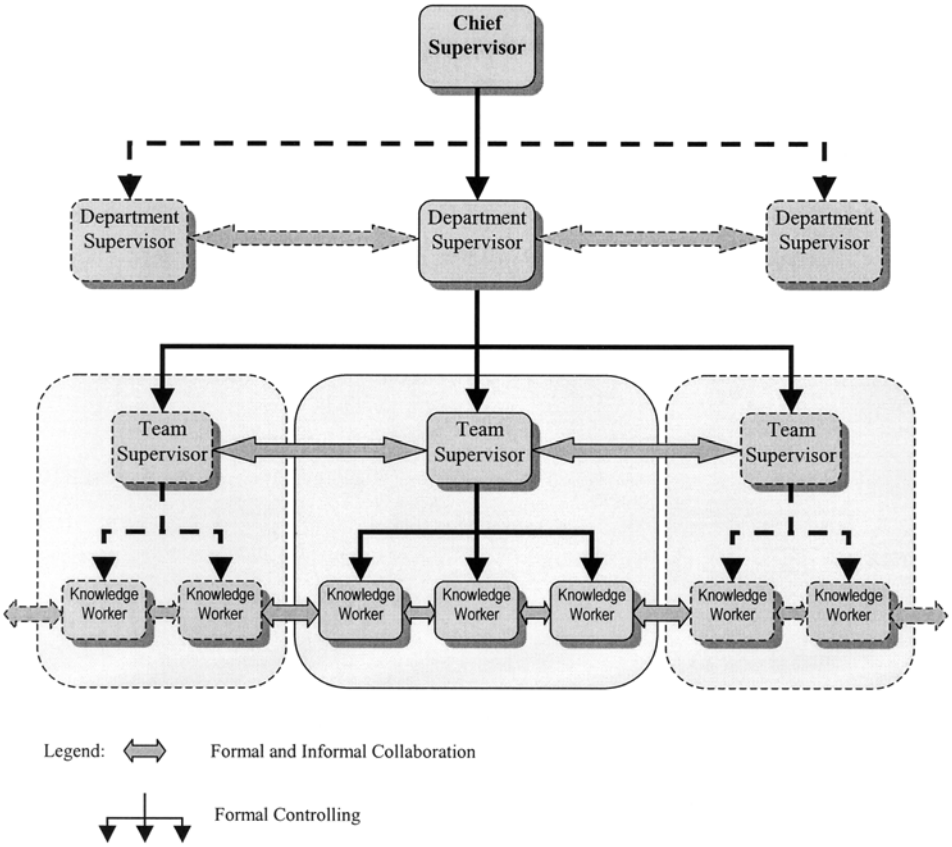


Figure 8. Controlling and Collaboration in the VZS

After the succession to NATO, the Czech military adopted a formal model of the NATO intelligence cycle in order to meet standardization requirements; however, the organizational structure and intelligence procedures have not fully reflected the standardized collection coordination and information requirements management (CCIRM) model. To amalgamate the existing structure and standardized intelligence procedures, the VZS uses the following CCIRM system, illustrated in *Figure 9*.

Extant Procedures and Practices: Using Nonaka's interaction modes between tacit and explicit knowledge, one can begin to study how every organization creates, organizes, and formalizes its organizational knowledge. The possible interaction modes are illustrated in *Figure 10*.

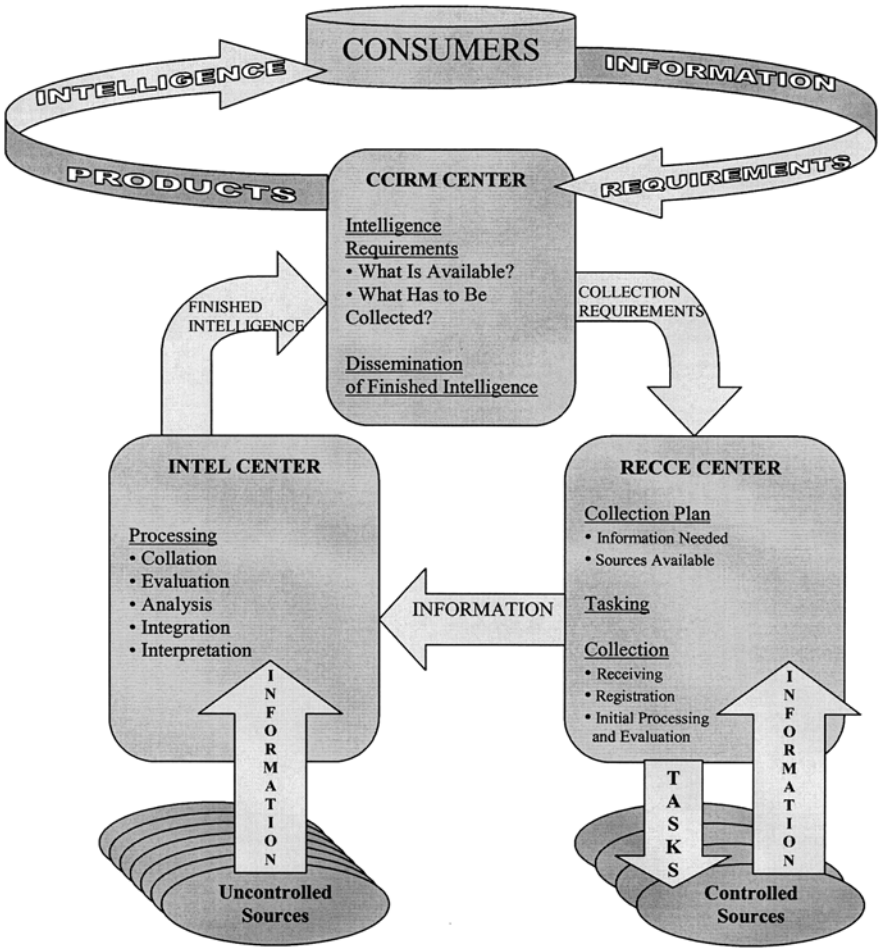


Figure 9. Collection Coordination and Information Requirements Management in the VZS

Although tacit knowledge held by individuals is the core of the knowledge creating process, full benefits can be obtained only when dynamic interaction occur through all possible modes—tacit to tacit, tacit to explicit, explicit to tacit, and explicit to explicit. As to the military intelligence, the actual intensity of the possible interaction modes is expressed by the thickness of the arrows. Most interactions are realized through the explicit channels, such as written orders and requirements, intelligence working papers, manuals, database exchange, or electronic communication. Then interaction also occurs between the tacit and explicit nodes, probably more in the direction from the explicit form to the human recipients. And the smallest portion of knowledge is actually

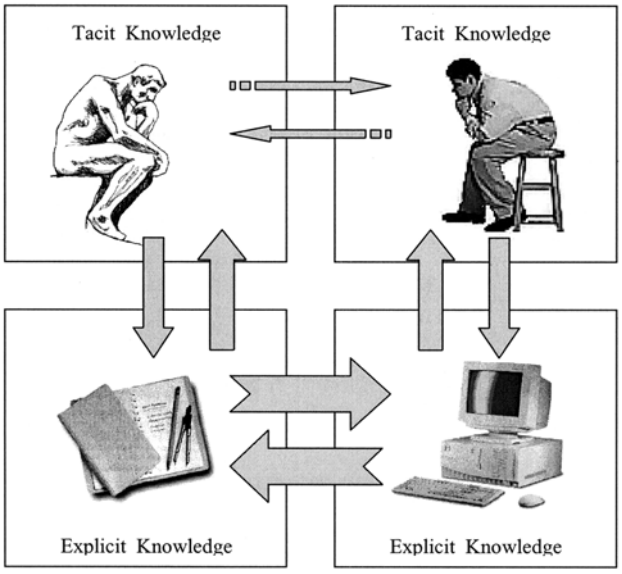


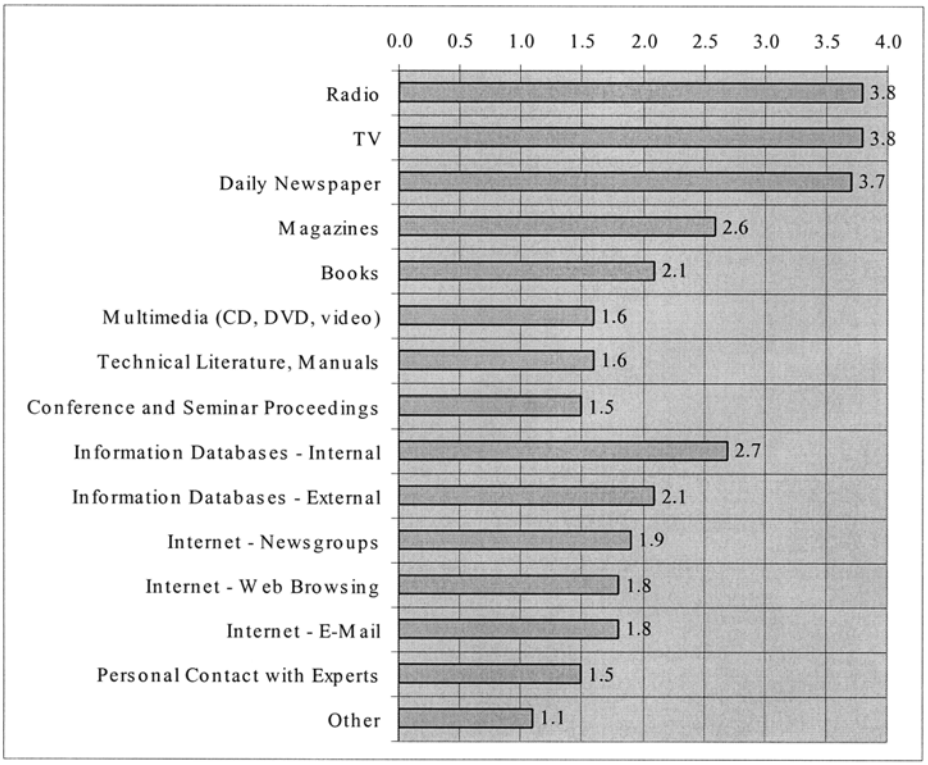
Figure 10. Military Intelligence and Knowledge Interaction Modes

exchanged through human-to-human communication, despite the fact that the tacit knowledge is probably the most important part of the organizational knowledge base, as already stressed.

To further quantify how often the VZS personnel uses each of the four modes of knowledge interaction, the representative sample of the VZS employees has been questioned. The following graphs express how often they interact with different forms of open sources.[17] *Graph 1* represents domestic sources; *Graph 2* illustrates the situation with sources abroad.

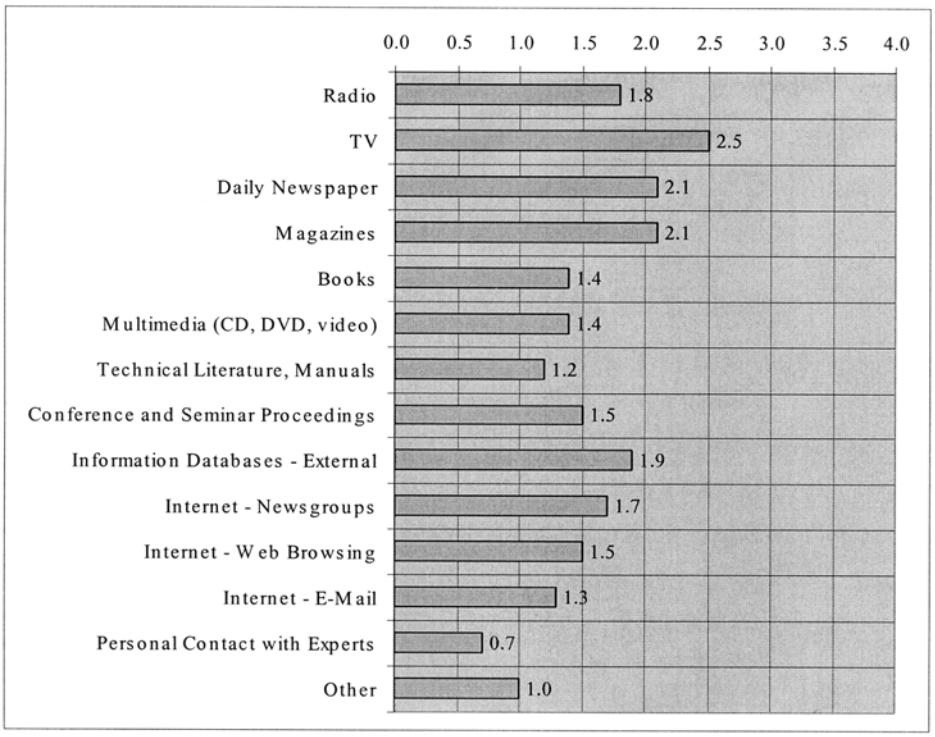
The knowledge created or captured in the OSINT seems to be based more on media and databases than on person-to-person contacts. This may be a result of many factors, such as source availability, language barriers, or budgetary restrictions. Further study will be definitely advantageous to future knowledge managers in the VZS.

[17] The frequency of use was graded as follows: 0—Never; 1—Seldom (at least once a year); 2—Occassionally (at least once a month); 3—Frequently (every week); 4—The most often (daily).



Graph 1. Frequency of the Use of Domestic Open Sources

As to the phase of knowledge formalization, the formalization of the knowledge does not occur systematically and regularly throughout the VZS. As the collected open-source data and information allow for creating new knowledge, this knowledge is frequently directly used during the intelligence process. To the author's best knowledge, the VZS has not yet employed any knowledge-based system (KBS) that could serve as a means to formalize open-source knowledge inside the organization. Existing information system is oriented toward information storage and exchange and can hardly serve to knowledge formalization. This is mainly because knowledge formalization requires that the knowledge management system be designed *after* the nature of knowledge itself is analyzed—not *before* or *without* such analysis. Unfortunately, intelligence managers and IT people often believe that a computer network can store human intelligence and experience.



Graph 2. Frequency of the Use of Foreign Open Sources

The formalization of knowledge also bears one negative aspect when it comes to the final fusion and production of the all-source intelligence. During the all-source analysis, the job of selecting and using appropriate knowledge is done twice—first, for open-source information, and then again with classified information. Current security apparatus is very restrictive as to channeling both classified and unclassified data into the same workstation. An extant information system does not allow automated merging of these two, owing to inadequate security measures. Data storage for classified data has evolved in a closed internal system, which is connected only to external systems of the same classification. This is certainly positive in terms of intrusion and computer attacks; however, it creates many "roadblocks" to all-source intelligence production.[18]

[18] Most interviewees estimated that the VZS uses 30-50% of open sources for all-source intelligence.

Distribution of knowledge both inside and outside the VZS is problematic, too. Knowledge based on classified information has its own specific distribution problems, as already foreshadowed. Knowledge based on open sources can be distributed freely; yet it seems as though *all* the information distributed and *all* the knowledge shared is tainted with the principle "need to know"—even unclassified information had to be registered until two years ago.

Estimated 75% to 80% of information is distributed on paper. As the existing electronic system does not provide for sufficient knowledge formalization, it cannot allow for knowledge sharing either. Printed lessons learned, handbooks, and intelligence manuals do exist; but they do not count for a significant part of the existing organizational knowledge.

It has been already stressed that knowledge should help individuals and organizations make decisions. In the VZS, the knowledge is applied mostly within the minds of individuals based upon the information set that is available at the moment. The knowledge base, which would help form one's decisions, does not exist. The OSINT center of the VZS has been redesigned recently, however, it seems to be established upon the traditional assumption—that OSINT is merely a counterpart, rather than a base, for secret collection. It is assumed that compiling data and information in a central repository can ensure that everyone with an access to the repository is capable of and willing to use it. This assumption is not valid. Most managers—the VZS not excluding—make decisions based on their interaction with others who they account knowledgeable about the issues. That does not signify that those accounted for the knowledge by managers are really the most knowledgeable persons. Without proper knowledge management, it is likely that managers will judge one's knowledge merely on one's glibness rather than on one's actual contribution to the organizational knowledge.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ADAPTING KNOWLEDGE MANAGEMENT THEORY TO THE CZECH MILITARY INTELLIGENCE

Knowledge work is the core business of the military intelligence. As stressed beforehand, knowledge work is not limited to the VZS; virtually all organizations across all the governmental and private sectors are becoming knowledge intensive (Drucker 1994). The Czech military cannot avoid this development; the Czech military must rather adapt to it. Today, the massive flow of open-source information overwhelms the traditional collection and analysis system that the military intelligence uses. Information is lost or wasted and even critically important information, when acquired, is not always turned into "corporate" knowledge. To achieve a working synthesis of IT and different knowledge domains, OSINT requires multi-disciplinary expertise, collaboration, and mutual learning. New models, leadership commitment, and new ways of thinking are needed.

This chapter outlines the main aspects of the OSINT knowledge system and process design for the Czech military. The first section presents the major steps to building knowledge management, focusing on the main areas to which the Czech military, particularly the VZS, should pay attention when designing its future OSINT. Then the second section of the chapter discusses the objectives and limitations of the OSINT process and system design. Finally, the last section encapsulates the OSINT process and system design and presents the general alternatives to the OSINT knowledge-management system.

A. MAJOR STEPS TO BUILDING OSINT KNOWLEDGE-MANAGEMENT SYSTEM

Introducing knowledge management into the existing OSINT environment of the VZS is a long-term task that should be built in incremental steps. Karl Wiig (1999) introduced sixteen building blocks that should be considered for introducing a new knowledge management practice. Based on his work, the following section describes

seven basic steps in their approximate order of implementation that the VZS should take when designing its OSINT knowledge-management system.

Management Commitment: Management commitment is essential for all the knowledge management efforts. Knowledge management champions among the top VZS leaders are needed to help create a shared vision of how the OSINT will be managed. Furthermore, both the leaders and the knowledge workers must develop a mutual conviction that knowledge management is the proper way to conduct OSINT. They must believe that it is worth their effort. To do so, well-founded, specific, relevant and realistic examples must be created to present the new knowledge-management opportunities to both the management and knowledge workers. That does not necessarily mean that the VZS must create such examples by itself first; many good examples of efficient open-source knowledge management can certainly be found in the business world and in academia, too.

Knowledge Mapping: Knowledge maps and similar surveys must first and foremost provide the understanding of the OSINT knowledge state. Such maps will describe major OSINT-related knowledge assets, activities, and practices, and will compare them to existing assets outside the VZS. Existing knowledge assets must be carefully mapped and collated with the directions and tasks assigned to the military intelligence. The VZS management needs OSINT knowledge mapping to establish the groundwork for a knowledge strategy and to identify specific needs and opportunities.

Owing to limited budgets and other restrictions, the VZS may not want to hire an external survey team to map the knowledge inside the organization. So, the VZS should build one or a few dedicated teams by itself to survey quickly and economically the existing open-source knowledge and to create OSINT knowledge maps. These maps will help propose actions the VZS management and knowledge workers must take, and the maps will also help define key OSINT requirements.

Knowledge Strategy: The VZS is an organization large enough to need a formally formulated OSINT strategy. A knowledge strategy is needed to determine how OSINT

will support the overall knowledge management, to set knowledge management priorities, and to determine key knowledge requirements, i.e. critical success factors (CSFs). The purpose of the strategy is to outline OSINT objectives by reflecting the knowledge management vision in a consistent framework. An explicit strategy will help OSINT managers and knowledge workers create and select specific solutions fitted to current and future conditions inside and outside the VZS. The strategy can improve decision-making by establishing a consensus around long-term goals, and by creating a vision for the OSINT knowledge workers. A strategic plan for OSINT should comprise at least the following elements:

- OSINT vision;
- List of the goals with regards to OSINT;
- Forecast of developments in the external environment to which the VZS must respond;
- Statement about how the VZS will extend its current OSINT system in the future;
- Actions and milestones regarding decisions and projects, including milestones and financial projections.

Key Knowledge Acquisition: Key knowledge must be acquired to fulfill the requirements of the CSFs. Here the focus is to obtain and to characterize the detailed open-source knowledge that will meet the CSFs demands. This can be done by gaining information from various open sources that will describe the actual knowledge in sufficient details for communication to other people and knowledge repositories. Using previously generated knowledge maps, knowledge workers can acquire the desired knowledge from individuals inside the VZS. Especially when employees are promoted or when they leave the organization, others should capture their valuable knowledge for reuse. Lessons learned, training, apprenticeship, and many other knowledge engineering methods are available to elicit extant knowledge. Furthermore, when sources of knowledge are outside the VZS—which, considering the nature of OSINT, will be the most frequent case—that knowledge must be gained for incorporation to the VZS knowledge assets.

Knowledge Transfer: Once the key knowledge has been obtained, it must be transferred to its users. Information technology (IT) itself does not manage knowledge, but it can greatly help the knowledge management process. It is important that the military management does not perceive knowledge management as just another database or a software program. These are just tools that support knowledge content. No system does it all; hundreds of products have different supporting functions, such as information search and retrieval, categorization, knowledge formalization, and distribution. The IT support personnel do not choose or create knowledge and its content. But they have the difficult task to select carefully commercial off-the-shelf (COTS) products that will support knowledge management well. The VZS must build a comprehensive knowledge transfer system by creating an expert OSINT network, consisting of experts online, expert software systems, intelligent software agents, and so on. Usually, the extant knowledge transfer systems follow traditional paths and are uncoordinated. Also, some parts of the expert network may be missing in the existing organizational structure and procedures, owing to limited budgets and deficient incentives. It is likely that such inefficiencies will be discovered during the process of knowledge mapping; so in this stage, the builders of the expert OSINT network must address them. Detail studies of commercially available IT tools will be necessary prior to selecting COTS hardware and software, as well as training programs for those who will use them. Following this, the expert OSINT network will serve its purpose—to make the knowledge possessed by individuals available for distribution to the VZS employees and customers.

Incentive Programs: VZS managers should motivate OSINT personnel to act intelligently—to be innovative, to capture new knowledge, to share their knowledge, and so on. Soon after the VZS management decides on a vision for OSINT, and after knowledge mapping indicates any needs for incentives or for removal of disincentives, the OSINT leaders can construct incentive programs in order to make OSINT knowledge workers personally responsible for knowledge mindfulness. The VZS management should know which factors influence behavior of OSINT personnel both positively and negatively and discuss these factors personally throughout the organization. Such factors may be associated with insufficient time or manpower, with people's self esteem, values

and emotions, with job security and social support, and so on. Because of the complexity and importance of such factors, the incentive programs must be continuous and flexible.

Knowledge Assets Facilitation: Knowledge assets, both tacit and explicit, must be carefully managed through all six phases of the knowledge management life cycle, using extant IT tools. A proper distinction between knowledge assets that are owned by the VZS and those existing outside the organization, together with balanced investments for these two asset categories, can help build and exploit knowledge assets, provide essential support, and steer the desired OSINT activities. When building or improving the expert OSINT network, all the important knowledge "pathways" must be addressed. Ideally, the OSINT system will provide functions for all the KMLC phases—not only for knowledge organization, formalization, and distribution, but also for knowledge creation, application, and evolution. Moreover, the network must allow consistent knowledge asset management at every level of the VZS.

B. OBJECTIVES AND LIMITATIONS TO BUILDING OSINT KNOWLEDGE-MANAGEMENT SYSTEM

This section synthesizes the objectives of the OSINT knowledge management process and system design and the major limitations that are likely to occur during the design process. After presenting the core issues of the knowledge management process, the key points of the organizational design are compiled. In addition to that, the section also pinpoints three challenges specific to the Czech military intelligence.

1. OSINT Knowledge Management Process

Understanding the objectives and limitations of the knowledge management life cycle in the Czech military is a necessary condition for designing a future OSINT knowledge-management system. The core issues of knowledge creation, sharing, and distribution are as follows:

Knowledge Creation: Creating new knowledge does not come automatically. It is typically an act of establishing a meaningful relationship between concepts or objects that have not previously been related. It could happen by a fortunate accident, or it could be a result of an appropriate organizational environment that fosters creativity. Creativity also requires certain personal qualities, such as curiosity, imagination, assertiveness, self-confidence, risk acceptance, and so on. The VZS certainly does not need castle-builders, but it may need visionaries and creative people. Intelligence personnel need to recognize when intelligence analysis may be no more sophisticated that existing "conventional wisdom" on a given issue, but they also need to recognize when "common sense" does not work properly and a non-conventional approach may help.

Motivating creativity in OSINT is certainly challenging. The most important aspects are developing communication networks and also a culture with freedom of thought and enjoyment in the performance. These aspects have certain organizational implications for OSINT that are summarized as follows:

- Organizational structure is flat, without hierarchical control, with task-oriented teams;
- Intelligence processes are directed toward generation, selection, and use of knowledge, with flexible planning and loose control;
- Reward system allows autonomy of individuals and recognition of their abilities;
- Knowledge workers elaborately combine technical knowledge with creative personal characteristics while managers act as sponsors and facilitators. (Galbraith and Kazanijan 1986)

Some of the implication listed above, especially those going against traditional hierarchy, are hard to imagine and extremely difficult to promote in the military. Yet, these are desperately needed, if the Czech OSINT should reach its fully creative stage. Although it is unlikely that the military intelligence will reach ideal conditions for creativity, the VZS can certainly adopt some of the above-mentioned aspects to its structure and processes.

Knowledge Sharing: No matter how good the OSINT system is, unless it is directly tied to visible organizational benefits, the implementation of a knowledge-management system can result in negative attitudes, low returns on investments, and resistant behaviors of those who are supposed to use it. Many organizations started building IT systems for knowledge management before building the cultural and collaborative base for such systems. But the issues of collaboration are important. For example, when tasked to contribute with their knowledge, people often see the request as:

- Extra work (they are not paid for it);
- No benefit for them (they do not need to share);
- No benefit for the organization (they are not sure who will use the shared knowledge);
- Benefit for others but little value to them.

It is no wonder that with such attitudes and beliefs people do not want to share, and therefore to give away what they know and what they have learned, sometimes at great expenses. In reality, one does not lose anything by sharing knowledge; personnel still retain what they know. But practically, knowledge sharing depends on how much people believe in and value themselves and the others. (Coleman 1999)

Knowledge sharing must be encouraged by certain rewards. The VZS management should not be surprised that it will want to implement a new information system, and it may end up solving the compensation issues. Obviously, that purely financial motivation to share knowledge is severely limited under the extant fixed disbursement system of the Czech military; however, economic incentives are not impossible. Moreover, people also respond to motives other than financial, such as to high cultural and professional values shared throughout the organization. The assistance of human resource professionals may be useful in building knowledge infrastructure and IT support when the VZS managers want to overcome traditional procedures and believes, which often judge an individual's value only in terms of what and whom that person knows. The military intelligence will need to establish trust within its OSINT network, both inside and outside the organization, to be able to share knowledge. Such trust is tough to build—especially within and among the intelligence services, where secrecy, suspicions, and distrust have strong roots. However, OSINT is an arena where

one does not need to hide one's existence and interests; on the contrary, extended contacts and mutual trust are critical to knowledge sharing in OSINT. For these reasons, the OSINT leaders must build mutual trust, find common context, establish reasons for knowledge sharing, and provide the space to think and share.

Knowledge Distribution: One should clearly distinguish between the dissemination of information and the dissemination of knowledge. Many technologies currently used by the VZS and other Czech military organizations only provide access to data or information alone. This would work assuming that the users could understand the presented data or information so well that they could easily convert it to knowledge or assuming that the users already had the knowledge to understand and use the data directly. But such assumptions are usually not valid, as probably no one can be knowledgeable in all subjects and also, intelligence personnel do not have the time to learn about a new subject in detail when they are usually tasked to answer specific questions. So, consultants and expert systems are frequently needed if the intelligence questions are to be answered correctly.

One way to answer questions out of one's expertise is to locate an appropriate specialist, simply by selecting someone from a list of experts or by finding people who posses the expertise. Another way is to use an expert system—often complex computer software, usually interconnected with other expert systems, containing the experts' decision-making knowledge and allowing the knowledge to be effectively distributed to users. The reader may know of medical, legal, and other expert systems being successfully implemented in the business world. Indeed, expert systems are not remedies for all the OSINT needs. Sometimes immature, expert systems are just as good as the people who created them, yet they are still behind any human specialist in terms of the ability to create, to share, and to use knowledge. However, expert systems can be an excellent solution for both intelligence analysts and intelligence consumers in many cases.

2. Organizational Design

Many managers in the Czech military believe that redesigning a system is creating new organizational charts and regenerating the tables of personnel and materiel. Yet, defining the future OSINT structure is definitely more complex than that. Here are the key points of the organizational design that must be considered during the OSINT design process:

Hierarchy in the Organizational Design: Complex organizations, such as the military, traditionally approach their needs for specialization, coordination, and cooperation by creating hierarchical structures. As Max Weber (1968) described decades ago, bureaucracies with their hierarchical structures, with coordination and control through rules and standard operating procedures, and with separation of jobs and people eliminate most of the natural human behavior—cooperation, innovation, personality, variation, and emotion. Contrary to these structures, often called *mechanistic* structures, an organization can adopt an *organic* form of its structure—a form that has less narrowly defined tasks, all-directional communication, widely dispersed knowledge, and people loyal to the organization and its goals, rather than to their immediate supervisor.

In the military, seemingly, no alternatives to hierarchy exist. As long as there are benefits from division of labor and specialization, hierarchy is inevitable. But the important issue is how the hierarchy should be structured and how the different parts of it should be related to one another. As shown in the previous chapter, the VZS is currently identified with an administrative hierarchy, in which the members are organized along superior-subordinate lines. Problems occur when the bureaucratic system with its standard procedures and high level of specialization has to produce various outputs from various inputs, using poorly implemented IT in a changing environment. The intelligence process can be jeopardized when the flow of information up the hierarchy and the flow of decisions down the hierarchy are too slow. So, the VZS should reorganize its OSINT structure to increase responsiveness to external changes. Although different branches and sections of the VZS can reach open sources with certain degree of independence from other subsystems, loose bonds of OSINT elements, equipped with more sufficient means

for communication and coordination will certainly increase the effectiveness for the whole VZ. Several factors urge the OSINT to move "beyond bureaucracy":

- The centralized, structured organization cannot readily adapt to change; to be responsive to external change, OSINT needs to be decentralized, with less specialization, and looser control.
- The information revolution changed the conditions for efficiency. Administrative bureaucracy and information systems to control people, as well as highly specialized manual labor, are less needed. Now, computer-integrated knowledge work and job flexibility are priorities.
- Decision-making power is needed at the operational level and should be accompanied by curtailing top-level staffs.
- To improve cross-functional cooperation, teamwork must be emphasized as the basis for organizing separate intelligence activities.

Designing OSINT Elements: If the OSINT system requires some form of hierarchy of its subsystems and elements, it is important to decide how the individuals are to be formed into teams and units within the VZS. For example, the OSINT elements can be organized on the basis of common task where the employees and assets are grouped according to their principal roles—information collectors, intelligence processors, communication specialists, and so on. The VZS might also develop its OSINT structure along the OSINT process itself, having separate elements for OSINT planning and direction, collection, processing, and dissemination. Or the VZS can organize its OSINT personnel according to their final products, such as OSINT daily monitoring awareness summary, all-source daily intelligence briefing, or monthly intelligence summary. Finally, OSINT elements can be grouped along their actual geographical location—or along the geographical location they pay attention to, such as the Balkans, the Middle East, or Russia. To decide properly, the military intelligence leaders must first understand the benefits and disadvantages of organizing the OSINT elements on one basis compared to an alternative basis, and then, when possible, combine the best of all the systems to design the organizational structure and management system of the future OSINT.

A critical design issue is the optimal degree of job specialization. Increased specialization certainly increases efficiency, but it also increases the need for coordination.

For example, the VZS can organize its OSINT knowledge workers into small cells—OSINT units. These units can consist of one or a few people according to the desired specialization, geographical location, and so on. Instead of a highly top-down controlling structure, the OSINT units can be organized rather loosely. Knowledge workers can then cooperate more easily both inside the OSINT unit and with other units through information networks and other IT tools. A rather loose organization structure of OSINT units is expressed in *Figure 11*.

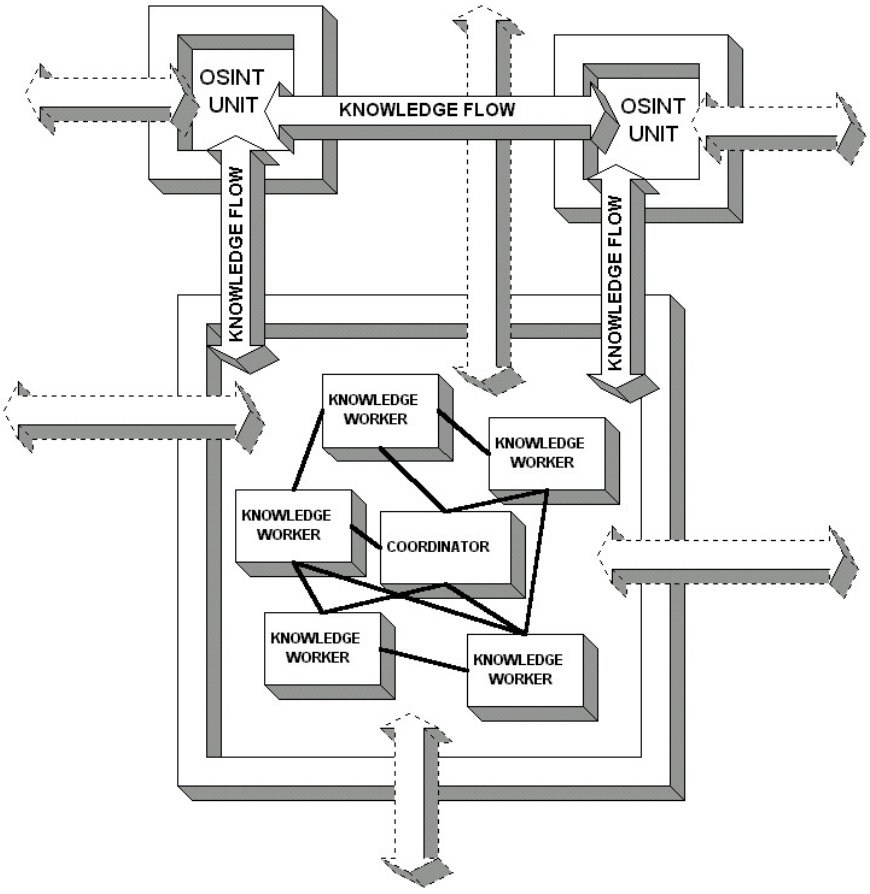


Figure 11. Loose Organization of OSINT Units

Coordination and Control: Coordination is vital to the organization's performance. The VZ specialists may be the best in the world—but unless they can coordinate their effort, their output is less than useful. Coordination in the VZ is not a technical issue; it is an issue of cooperation among different members of the organization who have different goals. Technology can just link those individuals and empower them to perform their tasks more efficiently. Coordination is mainly about establishing the knowledge-management system and procedures than can permit OSINT specialists, i.e. knowledge workers, to relate to one another and to adjust their individual actions. Three different mechanisms are basically available for achieving goal alignment within the VZ: *control mechanism*, *reward incentives*, and *shared values*.

Control Mechanisms typically consist of a manager supervising a group of subordinates. The manager monitors the subordinates' behavior and performance, and the subordinates are required to ask for approval when their actions are outside their reference. The incentives to comply with the existing hierarchy are both positive—promotion up the hierarchical ladder, and negative—no promotion or dismissal. Control mechanisms are demanding in terms of several layers of supervisors that are needed to conduct the functions of monitoring and coercion. This mechanism would probably be efficient in situations where the knowledge workers would systematically use extant knowledge to produce standard output—similarly to workers in a production line. It is doubtful that such a situation would be the usual knowledge work in the VZS.

Reward Incentives involve rewarding one's actual performance. Such incentives directly link rewards to output, which is highly desired. Moreover, this mechanism significantly reduces the need for a costly management structure. However, this may be challenging in terms of performance measurements. Military intelligence specialists should not be rewarded according to the number of pages they produce on intelligence; they also should not be rewarded for how many hours they spent at work. The VZS employees do not work on machines producing nuts and bolts; they are supposed to create and use knowledge. Regular, even real-time adjustments and feedback to knowledge workers would help them take full responsibility for their work, without the necessity for supervisors. The key to promoting effective cooperation is to have more

sophisticated incentives than just the threat of dismissal or of losing a promotion. Obviously, establishing accurate performance measurements—so that a person can be rewarded for his or her actual knowledge performance— requires profound studies by experts.

Shared Values can be rewarding by themselves when the organization's goals are conflict free. Then, the VZ can achieve high levels of cooperation without extensive control mechanisms and without performance-related rewards. Unfortunately, the organization's goals are generally not conflict free, and such a mechanism is effective only in small teams that consist of highly devoted members of the intelligence community. Yet, this type of mechanism should not be forgotten because individuals who are driven more by their moral and ethical values than by their pay do exist and are often superior employees. Professional intelligence culture, comprising of positive beliefs, values, and behavioral norms can certainly influence how the VZ employees think and behave. Indeed, organizational culture takes a long time to develop and cannot be changed easily. However, open-source environment does not need to be wrapped up in mysteries and secret intelligence games, thus the organizational culture can serve as a unifying factor for cross-functional OSINT teams.

One way or another, the future OSINT structure in the Czech military should provide for both a team-based and a project-based network of open-source experts, who will be available both inside and outside the VZ. Such a network can be flexible and responsive to various OSINT tasks, if the VZ focuses on coordination rather than on control. The OSINT knowledge-management system must permit knowledge to flow both vertically and horizontally. A well-balanced combination of the possibilities mentioned above is needed if the knowledge assets in OSINT are to be employed effectively.

3. Challenges Specific to the Czech Military Intelligence

Common challenges for knowledge management and OSINT have already been mentioned throughout the thesis. But the Czech governmental intelligence services, such as the VZ, also have to face other specific challenges.

First, the VZ must strictly obey the laws and regulations related to vetting of its personnel and to handling classified documents. In author's opinion the Czech Republic's laws and regulations in this area exceed any practical needs while often creating serious problems for individuals and organizations that must meet these formal requirements. Also, the "secrecy games" often limit, if not prevent, sharing of information and knowledge and additionally narrow the amount of people who can participate in the organizational knowledge sharing and decision-making processes. In scientific work, secrecy hinders the advancements of knowledge; in military strategy and tactics, secrecy can prevent careful planning and implementation of projects. Secrecy also obstructs reasoning, limits the perception of the problem, and limits alternatives to solving the problem, thus restricting choices and decisions (Bok 1983). Fortunately, OSINT need not be encumbered with such restrictions. The military personnel dealing with OSINT may certainly be the same people who deal with secrets. It just takes a specific mindset, as well as training and practice, to distinguish properly between unclassified and classified information when necessary and to amalgamate the two when needed.

Second, information attained by the intelligence service is usually stored for a long period of time in order to provide for long-term analysis. However, the amount of information accessible from the open sources largely exceeds the amount collected covertly. Moreover, the dynamic nature of open sources does not support simple storage of data or information gained via OSINT, as they could easily become obsolete. So, rather than store everything in the OSINT cycle, OSINT collectors, analysts, and managers will have to carefully consider the relevancy of information and intelligence products and use the IT tools at their disposal cleverly.

Third, many documents must exist on paper. Although automated document processing is not a new concept, the VZ and other military organizations still require documents on paper, mostly signed by the top commanders and directors. (The higher, the better.) A secure electronic document exchange would speed routine daily work tremendously. Unfortunately, most military personnel still trust paper more than computers, although the paper is usually not a qualitatively higher form of information storage and bears many limitations that electronic systems do not have. Currently, with increasing concerns about information security (INFOSEC),[19] the Czech military tends to be quite cautious about using computers and information networks. However, the Czech military can ensure necessary data integrity and availability through the smart use of modern technology for INFOSEC, such as the virtual private network (VPN), the Secure Sockets Layer (SSL), and many other techniques.[20] Indeed, collaborative computing may have its strict limitations in classified matters; but with OSINT, the military need not be so concerned.

C. OSINT KNOWLEDGE MANAGEMENT PROCESS AND SYSTEM DESIGN

This section presents an alternative model of the future OSINT knowledge-management system of the Czech military. First, the section discusses the use of IT in general, and four main IT tools that should be employed in the Czech military OSINT—intelligent agents, knowledge repositories, groupware, and expert systems. Then, a general model of the OSINT knowledge-management system is designed.

[19] Generally, INFOSEC covers everything that is related to information systems security—personnel security, physical security, operations security (OPSEC), communication security (COMSEC), computer security (COMPUSEC), emissions security, and so on. INFOSEC issues for OSINT represent a field for a separate specialized study.

[20] Data secrecy, data integrity, and data availability are three objectives of information security (INFOSEC). Data secrecy is of no concern in OSINT. However, data integrity, i.e. prevention of unauthorized modification and assurance of data accuracy, as well as data availability, i.e. timely response of the system, are important parts of the OSINT knowledge management system design.

1. Facilitating Knowledge Flow

Military intelligence analysts, as well as decision-makers, can frequently answer their own questions using open sources. To do this effectively, they need IT tools that will allow them to find the desired knowledge, as well as to store and to share the knowledge they already posses. As stressed before, the Czech military must adapt to changes and requirements of the outside environment, partially by improving IT. Today's information technology allows one to capture and to store OSINT knowledge and to disseminate it throughout the organization. The Czech military must take advantage of extant IT to codify tacit knowledge, store it, and make it accessible to others.

The future IT infrastructure of the VZS should provide as much functionality as possible. Here are just a few examples of what the IT infrastructure can provide to support the OSINT knowledge-management system (Wiig 1999, Nissen et al 2000):

- Information gathering and information exchange through E-mail, intranet, Internet/WWW;
- Internet/intranet data/information gathering through intelligent agents ("bots");
- Collaboration through groupware;
- Knowledge maps and knowledge "yellow pages" on intranets;
- Access to knowledge base systems/expert systems;
- Automatic pattern matching and inference from databases;
- Knowledge creation tools for discovery in databases;
- Knowledge organization and formalization tools;
- Global knowledge distribution and sharing;
- Office automation and management functions;
- Distance learning.

In the following, four main IT tools that should be incorporated in the future OSINT system in the Czech military are discussed.

Intelligent Agents: Intelligent agents are computer programs that can autonomously perform some human-like tasks and act on behalf of their users. These agents mostly integrate, analyze, evaluate, and interpret collected raw data; so they do not perform any knowledge-management functions, but they are certainly useful by automating the data processing and exploitation. Most readers have probably already used intelligence agents, in one form or another, when searching for information on the Web. Obviously, intelligent agents can be employed in various areas of the military intelligence functions. For example, they can be used to interact with an OSINT knowledge base, to determine how the given task can be fulfilled effectively, and to perform the necessary actions to reach the desired goal. Intelligent agents, connected with sensors on reconnaissance assets and performing automated tasks, can serve as other examples. Either way, the possible employment of intelligent agents should be carefully studied in order to decide about their applicability to the Czech military OSINT.

Knowledge Repositories: Knowledge repositories can capture and formalize knowledge in its explicit form for further use throughout the VZS. Two basic types of knowledge repositories are

External knowledge, which refers to knowledge about entities outside the VZS;

Internal knowledge, which could be either structured, in a form of intelligence summaries, intelligence manuals, and so on, or informal, e.g. discussion forums, lessons learned, and so on. (Davenport et al 1998)

As explained in the previous chapter, the military intelligence deals with all forms of knowledge—tacit and explicit, external and internal. So, knowledge repositories can certainly be used in the future OSINT system in order to provide basic platform for transferring the tacit open-source knowledge from individuals into a knowledge repository. The VZS should employ a nation-wide electronic discussion system as a part of its knowledge repository, through which it will be able to access experts outside the organization. The VZS should also build electronic OSINT knowledge repositories to perfect the knowledge transfer and knowledge internalization processes. The OSINT knowledge repositories must be made available through electronic networks to the

military units, especially when they are deployed in the military operation during a crisis or in humanitarian relief.

Groupware: Groupware techniques allow individuals to communicate and collaborate with high efficiency by providing rich content and interactivity through real-time presentations, electronic boards, discussion forums, and video conferencing. This overcomes problems with dispersion of the military personnel in time and space and also avoids some of the negative aspects related to turnover of personnel and lack of face-to-face communication. Groupware can significantly help OSINT personnel participate remotely in the intelligence cycle processes. Moreover, groupware helps orient newcomers, familiarize them with procedures within and outside the intelligence community, and supports transitions of the organizational practices from one person to another (Davenport et al 1998). While such knowledge is relatively easy to capture and store, it will be difficult to find and to use without proper indexing and searching tools (Oxendine and Nissen 2001). The VZS should utilize COTS groupware, such as Lotus Notes, to facilitate the capture and the exchange of tacit knowledge. Moreover, the use of groupware must be accompanied with proper incentives for the VZS employees, as well as for the people outside the organization to contribute and to share OSINT knowledge.

Expert Systems: Expert systems (ES) are computer programs that help non-experts make decisions similar to those of experts through an emulated interaction with a specific expert domain, such as finance, history, electronics, law, medicine, and so on. When communicating with the ES, users usually have no or limited knowledge about the subject but the ES supplies a part of an expert's decision-making knowledge through knowledge capture, storage, and dissemination. An expert system basically consists of a knowledge base and a capability to inference, which is provided by "interactive" communication between a user and the ES. By asking questions, making recommendations, following the Yes/No decision trees, and so on, the ES can play an important role in the OSINT knowledge-management system.

The Czech military should use outside expert systems intensively, as well as create a military intelligence expert system on its own. Especially in the times of crisis, or

when the troops are deployed far from the direct intelligence support of the VZ, finding a specialist and communicating face-to-face can be hard to arrange. ES can assist commanders and staffs in the field to evaluate and interpret open-source information, help them recognize threats and trends, and support commanders' decisions.

Indeed, creating an OSINT expert system is not a trivial task. First, the VZS must capture and formalize the necessary OSINT knowledge to create a knowledge base. This part is many times the Achilles' heel, for the ES developers must choose a proper set of knowledge-engineering tools and techniques and also knowledge workers must carefully fill the knowledge base with data—which is difficult and time consuming. Then, when the knowledge base is ready and the expert system is operational, future refinements are likely as the ES further develops. The expert system can serve, in the long-term, as an overlay interacting with the knowledge repositories that will be created in the short-term, looking for the relevant knowledge, and using it as a part of the ES decision support process (Oxendine 2000).

Figure 12 illustrates the incorporation of IT tools, and the way the IT infrastructure can help facilitate knowledge flow in the OSINT system. One should not perceive the four IT means outlined above as "either-or" options. All the means are applicable to the OSINT knowledge-management system in the Czech military—but the means differ in their sophistication and complexity, budgetary demands, and implementation time.

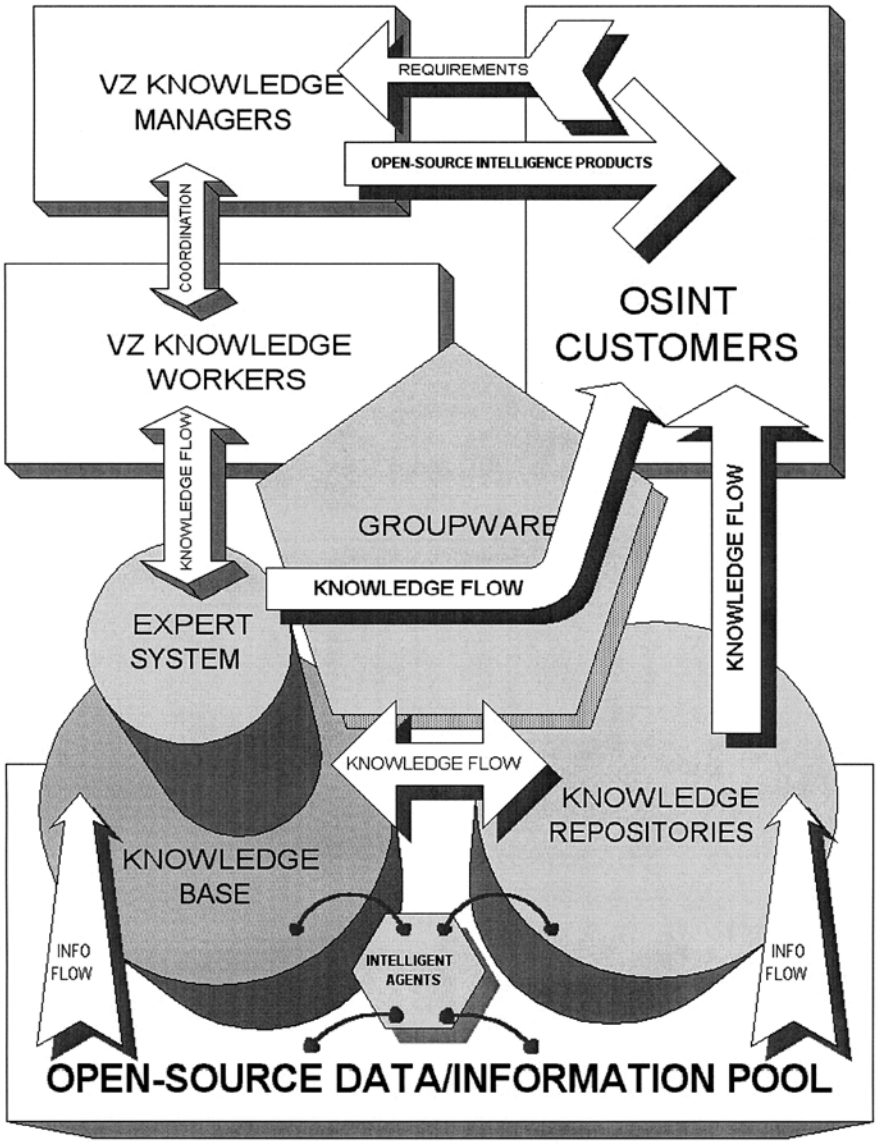


Figure 12. OSINT Knowledge Flow and IT infrastructure

2. Organization of the OSINT Knowledge-Management System

Jansen's contingency model, introduced in Chapter III, helped define the current organizational design of the VZS as a mixture of two types—division into business functions, and division into domains. The extant organizational design and IT does not reflect the characteristics of the modern open-source environment, which is perceived as highly complex and highly variable. In such an environment, the knowledge of each element of the organization is no longer sufficient to manage this knowledge. In order to manage this knowledge, the VZS should organize its OSINT structure to allow interpreting implicit knowledge, as well as to link old knowledge with new knowledge, thus creating new knowledge again. This is called *combined capacity* (Jansen et al 2000). The VZS should build mechanisms, such as knowledge repositories and groupware, to bond the compiled knowledge and to provide for its distribution and reuse.

Building upon the Jansen's contingency model, one can see that the VZS organizational design should migrate toward creation knowledge through increased combined capacity of OSINT units, as depicted in *Figure 13*.

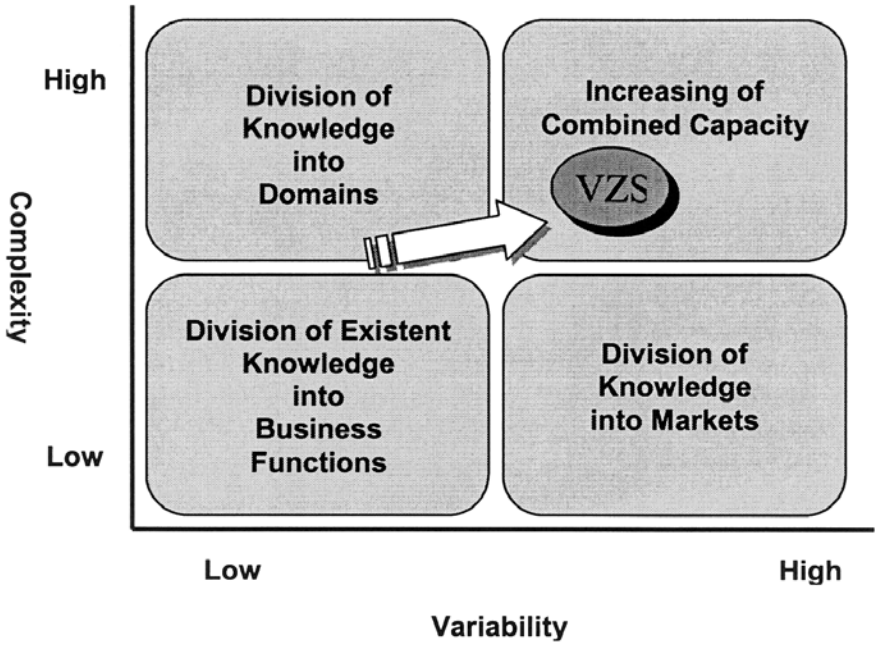


Figure 13. Four Strategies for Knowledge Management and the Future VZS

The increase of combined capacity is the only way to create new knowledge out of existent knowledge (Jansen et al 2000). If the military intelligence wants to maximize the combined capacity in OSINT, it must explore new forms of work, minimize rules and procedures for OSINT, and allow the highest possible degree of freedom for OSINT knowledge workers.

The new organizational design of the VZS and its information and communication technology should reflect the characteristics summarized in *Table 2*.

Organizational Type	Organizational Design	IT and Communication
Increase of Combined Capacity	• Organizing in Projects • Little Control, Much Freedom • Virtual Organizational Structure	• Informal System Focused on Knowledge Creation • Intranet/Internet, Intelligent Agents/Search Engines, Groupware, Expert Systems

Table 2. Characteristics of the Future Organizational Design and IT in the VZS

The new OSINT knowledge management system does not need to dispose of old practices—as long as the practices sustain continuous reexamination and prove to be the best practices. Similarly, not everything that is newly created represents a better alternative to the knowledge already existing. Hence the VZS should build its OSINT knowledge-management system to balances efficiency—by propagating and disseminating extant knowledge—and flexibility— by creating and renewing knowledge.

Virtual OSINT Organization: As mentioned in the previous chapter, the current organizational structure resembles a traditional vertically oriented control with accentuated bottom-up knowledge flow while the daily life requires the VZS personnel to collaborate in the horizontal direction. OSINT—in comparison with other "INTs"—is much less limited than typical secret intelligence activities; OSINT managers can

certainly be pioneers in exploring new controlling strategies and in creating a modern OSINT structure.

One way to "organize" OSINT is not to organize it at all—at least in the traditional meaning. A concept of a virtual OSINT organization is very broad and is probably more limited by the people's will to accept such a notion than by extant IT means. A virtual OSINT organization can be a network of independent elements—OSINT units in the VZS, individuals and groups inside the Czech military, experts in academia, and so on—linked by IT to create, share, and distribute OSINT knowledge, as well as to share costs that are related to it. IT plays a central role in developing such virtual organization (Byrne 1993). A knowledge base in a virtual organization is widely distributed and this wide knowledge spread can enormously benefit all members of the virtual organization. The virtual model probably represents the highest flexibility in terms of timelines, responsiveness, and exploiting knowledge. Unlike the fixed organizational structure, such a broad virtual organization can easily modify its structure once the specific opportunity has been exploited or once the given task has been solved. Ideally, each element of the virtual OSINT "corporation" will cooperate in accordance with its core competencies. The partnership among the different elements will last as long as it is beneficial for the cooperating partners (Dees et al 1995). The whole structure will concurrently work on various issues through computer networks in real time.

Figure 14 illustrates a simplified vision of the virtual nation-wide OSINT organization. The main emphasis of the virtual organization is to complement and share resources in order to increase effectiveness and to lower costs. For small organizations or for organizations with severely limited resources—such as the Czech military—the virtual concept enables OSINT knowledge workers to join other organizations and to work on a much larger scale. In its maximal variant, the military, the police, academic researchers, intelligence services, other governmental bodies, and so on can create a nation-wide OSINT corporation that will be highly competitive internationally. The VZS does not need to be a dominant element of such nation-wide OSINT network—but it can certainly be the leader and the core of the OSINT network in the Czech military.

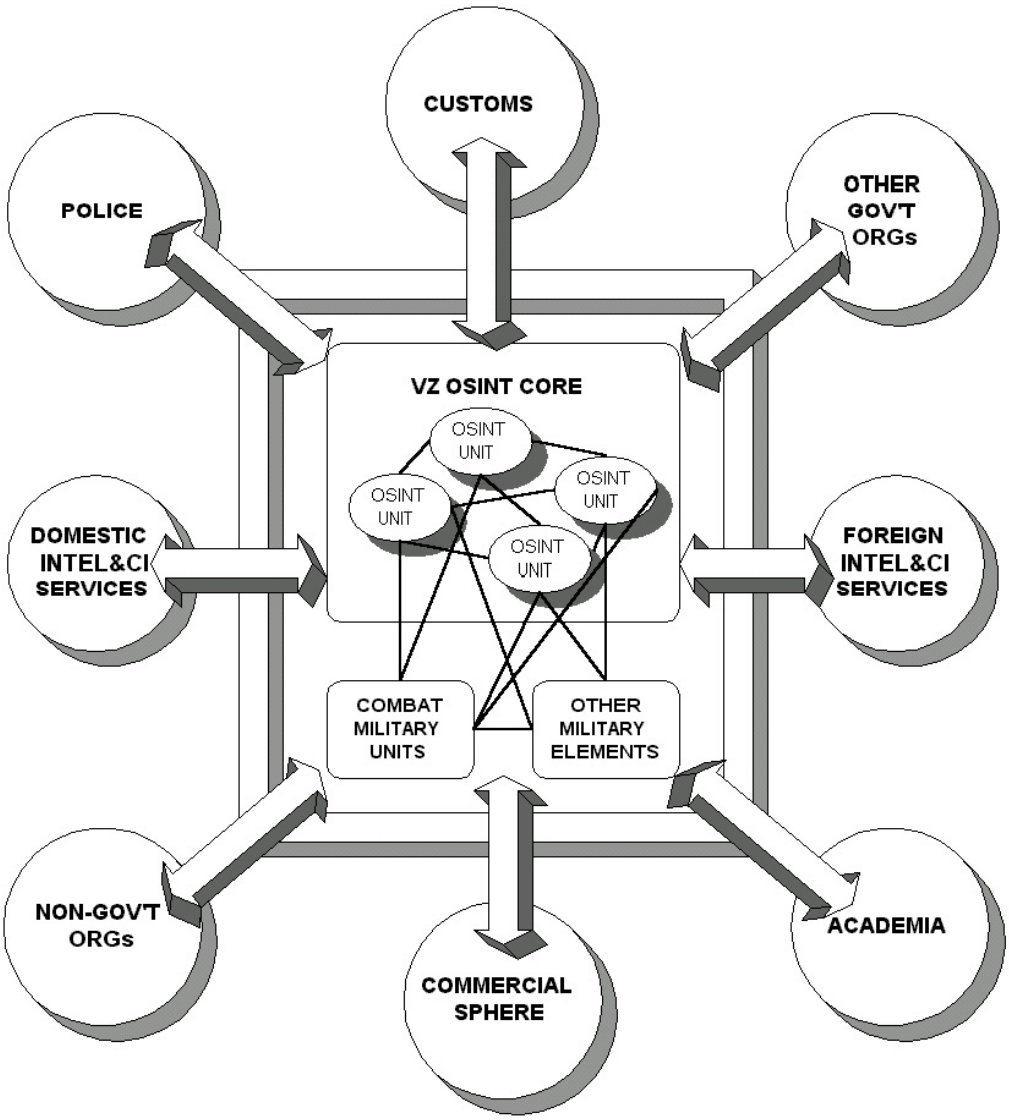


Figure 14. Virtual OSINT Organization

V. CONCLUSIONS AND RECOMMENDATIONS

This chapter summarizes the main points of the previous chapters. The first section of this chapter stresses the significance of system approach and summarizes the main steps that the VZS management should take. The second section underlines the multifunctional and cross-organizational nature of OSINT and the importance of a virtual OSINT network. The last section offers possible directions for further research and development.

A. SIGNIFICANCE OF SYSTEM APPROACH

Intelligence agencies are traditionally very conservative organizations. The Military Intelligence Service (VZS) management, as well as some of the knowledge workers may perceive changes to OSINT as a threat to the VZS and/or to themselves. Yet, improvements in the OSINT gathering and processing are not a threat to intelligence— reforms can ensure that a modern future for the Czech military intelligence exists. The Czech military intelligence should welcome all the advantages of modern open-source environment, which plays a highly important role in today's intelligence.

Today, as many individual organizations perform distinct intelligence tasks supporting an overlapping set of customers, deciding what an intelligence agency needs to collect is becoming more complicated. This is particularly true with OSINT, which is also influenced by the fact that Czech intelligence services now compete for resources. When using OSINT effectively, the military intelligence can respond to diverse crises efficiently and can also better allocate its severely limited resources into other areas of intelligence collection, when expensive covert means are unavoidable.

If the VZS wants to improve its OSINT, a systematic approach to the open-source domain is needed. As shown in this thesis, the VZS can design a modern OSINT for the Czech military by adopting knowledge management theory. The key point is that those who will devise the future OSINT knowledge-management system should systematically

follow the four stages of the knowledge system and process design—process analysis, knowledge analysis, contextual analysis, and systems analysis and integration. Systematically applying the knowledge system and process design will help achieve the objectives and strategies of the VZS, and pinpoint the knowledge required so that the organization can reach its objectives.

One must realize that the knowledge management system must be designed *after* the nature of knowledge itself is analyzed. Then, the knowledge within the VZS can be identified, captured, organized, formalized, and distributed throughout the organization. The VZS must develop knowledge maps to identify who possesses what kind of knowledge, both inside and outside its organizational structure. Moreover, the VZS must carefully survey its organizational design, focusing on controlling strategies and the information-flow configurations. Finally, the OSINT knowledge management designers must study each of the six phases of the knowledge management life cycle (KMLC) in terms of extant procedures and practices within the organization.

The VZS should gradually build a comprehensive knowledge management system by creating a virtual OSINT network, consisting of experts online, expert software systems, intelligent software agents, and so on, to make open-source knowledge available to the VZS employees and customers. Future OSINT network must support creativity, content-rich communication, and effective knowledge sharing.

A systematic approach will certainly require much effort and time, but the VZS will not be able to manage OSINT knowledge properly without this effort and without a long-term commitment. The systematic approach will identify existing open-source knowledge and capture it. It will also help find possible overlaps or inefficiencies in the existing or future OSINT knowledge-management system. This approach presupposes not only comprehensive knowledge about an adversary but also the ability to update this knowledge continually so that the military intelligence can react quickly to a changing situation. We have to move toward "situational awareness," which will depend on advanced information processing technologies, such as artificial intelligence, in order to fuse large quantities of open-source information into an accurate, real-time intelligence. Hence, OSINT must serve as a wide base for the other intelligence disciplines.

It must not be forgotten that the entire knowledge management effort will just be rhetoric without a management commitment. Knowledge management champions among the top leaders must envision how the OSINT will be managed, pursue the vision, and share it with others. OSINT managers and knowledge workers must believe that a modern knowledge-management system is the proper way to conduct OSINT, and that it is worth their effort. Such conviction is not implied—people must create it.

B. ORGANIZATIONAL ISSUES

Every intelligence organization should serve not only the highest levels of government but also the subordinate levels, where actions are taken on a day-to-day basis. Several intelligence studies, made by research organizations and governmental bodies (e.g. Gannon 2000/1, IC21 2000, Nissen 2001), showed that a major key to improving the intelligence community in the information age is the concept of "corporateness." That means, the VZS should function and behave as a part of a more closely integrated entity working toward a highly defined goal: the delivery of timely intelligence to various military and civilian decision makers.

The Czech intelligence community needs to manage knowledge smarter, finding new ways to do more with less. Rapid technological advances in knowledge management may offer new possibilities and advantages. The intelligence community should not ignore these advances—just as terrorists, proliferators, smugglers, information warriors, and other potential adversaries capitalize on such advances.

Owing to the information explosion, single analysts and analyst cells are not able to process all the available open-source information anymore. A robust OSINT knowledge-management system can save much time and resources, reducing unnecessary intelligence requests. The VZS must find ways to create and to maintain a virtual network of information sources, collectors, exploiters, analysts and customers, as appropriate, and maximize the productivity and responsiveness of individual analysts. The future OSINT organization should effectively and economically share resources.

OSINT is an intelligence discipline that allows the VZS to become a virtual, project-oriented enterprise. The VZS can adopt an organic, as opposed to a mechanistic structure—a form that does not have closely defined tasks. A rather loose organizational structure that emphasizes teamwork, all-directional communication, and widely dispersed knowledge can provide a desired environment for the future OSINT knowledge workers.

The VZS should not struggle to divide the OSINT elements into strategic and tactic levels, trying to follow the traditional military hierarchy. Once the OSINT elements are connected through electronic networks, all organizational levels de facto disappear, and the OSINT units work as parts of one large virtual corporation.

IT infrastructure will play an important part in the future OSINT system. The future IT structure should guarantee automated electronic document storage, retrieval, and exchange. Internal knowledge must be stored in the electronic knowledge repositories, and these repositories must be available through electronic networks. Groupware technology must facilitate the capture and the exchange of knowledge. Intelligent agents should be used to interact with open-source databases. A nation-wide electronic discussion system should provide access to experts outside the military. In the long term, the VZS should create a military intelligence expert system, which will be available to the military units, especially when they are deployed during a crisis or in humanitarian relief.

C. RECOMMENDATIONS FOR FURTHER RESEARCH AND DEVELOPMENT

This thesis establishes a base for the Czech military to employ modern knowledge-management theory and to build a future OSINT system. Further research and internal analyses are necessary to design the OSINT knowledge-management system. Moreover, as the knowledge process and system design is applicable to other intelligence disciplines as well, the VZS may want to analyze the other "INTs" in similar manner as the OSINT system.

First, the VZS may need a comprehensive study of its own tasks and capabilities to identify what knowledge is vital in order to assess performance in the VZS. After the study, each of the critical success factors (CSFs) should be evaluated as a single-target process. Then, the existing OSINT system must be evaluated in terms of process pathologies to determine how well the existing process meets the desired goals. Such a diagnosis will help eliminate the pathologies from the process. Also, the VZS should study how its employees utilize different methods of communication; here the assistance of human-resource professionals may be particularly useful.

Once the designers analyze each process in the extant OSINT system and design the future knowledge-management process, the VZS must reconsider its IT infrastructure. IT specialists must conduct thorough studies of commercially available IT tools and then select appropriate COTS hardware and software. The VZS should consider using intelligent agents and determine their applicability to the Czech military OSINT. All of this is certainly a complex task—random and rushed implementations of "IT solutions" into existing processes cannot work in both the civilian and military organizations.

Finally, the VZS must determine the future organizational structure of OSINT elements—yes, this is the last step, not the first one. The OSINT system designers must recognize the benefits and disadvantages of different bases, and then combine the best of all the alternatives to create the future organizational structure of the OSINT knowledge-management system.

Closing Thought: People, not machines, are the key element of the intelligence community. All of the collection capabilities would be meaningless without dedicated and well-educated people who know how to manage knowledge and how to use modern IT tools. The knowledge of many experts in the intelligence community who claim to know something about computers, software, and technology in general is still low. Few military employees have the insight to recognize adequate and inadequate computer technology. Although many employees have become more “tech-savvy” during the last ten years, continuous education and training is needed to move ahead, toward the world of open sources.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES AND WORKS CITED

Adams, J. (1998): *The Next World War*. Simon&Schuster, New York, 1998.

Allied Joint Publication No. 2.0 [AJP-2.0.] (2001): *Allied Joint Intelligence, Counterintelligence and Security Doctrine*. 2nd ratification draft. Military Agency for Standardization, Intelligence Working Group (MAS/INTWG), NATO HQ, Brussels, 2001.

Analysis of Required Capabilities, Target Structure and Composition of the Armed Forces of the Czech Republic (2001). Center for Preparation of the Armed Forces Reform, Prague, CZ, 2001. (Online) http://www.army.cz/reforma/english/dokument.htm.

Arquilla, J. and Ronfeldt, D. (eds., 2001): *Network and Netwars*: *The Future of Terror, Crime, and Militancy*. Santa Monica, CA, 2001.

Bok, S. (1983): *Military Secrets*. in: Derth, D.G. and Gooden, R.T. (eds., 1995): *Strategic Intelligence*: *Theory and Application*. DIA/JMITC, Washington, D.C. Second edition, 1995.

Buchanan, B.G. (2001): *Creativity at the Metalevel*. AAAI-2000 Presidential Address. AI Magazine, Fall 2001.

Burns, T. and Stalker, G.M. (1961): *The Management of Innovation*. Tavistock Institute, London, 1961.

Butler, R. (1991): *Designing Organizations*: *A Decision-Making Perspective*. Routledge, London, 1991.

Byrne, J.A. (1993): *The Virtual Corporation*. Business Week. February 8, 1993.

Clarke, R. (2001/1): *Fundamentals of Information Systems*. (Online) http://www.anu.edu.au/people/Roger.Clarke/SOS/ISFundas.html.

Clarke, R. (2001/2): *Knowledge*. (Online) http://www.anu.edu.au/people/Roger.Clarke/SOS/Know.html.

Coleman, D. (1999): *Groupware: Collaboration and Knowledge Sharing*. in: Liebowitz, J. (ed., 1999): *Knowledge Management Handbook*. CRC Press, Washington, D.C., 1999.

Cooper, J.R. (1997): *The Emerging Infosphere*. McLean: Science Applications International Co., Virginia, 1997.

CRS Report for Congress (2001): *Terrorism*: *Near Eastern Groups and State Sponsors, 2001*. Congressional Research Service, The Library of Congress, USA, 2001.

Davenport, T.H. (1995): *Business Process Reengineering*: *Where It's Been, Where It's Going,* in Grover, V. and Kettinger, W.: *Business Process Change*: *Reengineering Concepts, Methods, Technologies.* Idea Group Publishing, Hershey, PA, 1995.

Davenport, T.H., DeLong D.W., and Beers, M.C. (1998): *Successful Knowledge Management Projects*. Sloan Management Review, Winter 1998, in: Oxendine, E. and Nissen, M.E. (2001): *Knowledge Process and System Design for the Carrier Battle Group*. Knowledge and Innovation: Journal of the Knowledge Management Consortium International. Vol. 1, No. 3, April 15, 2001.

Davenport, T.H. and Prusak, L. (1998): *Working Knowledge: How Organizations Manage What They Know*. Harvard Business School Press, Boston, MA, 1998.

Dees, G.G., Rasheed, A.M.A., McLaughlin, K.J., Priem, R.L. (1995): *The New Corporate Architecture*. The Academy of Management Executive. Vol. 9, 1995.

Defense Science Board – DSB (1996): *Improved Application of Intelligence to the Battlefield*. A DSB Study, May-July 1996. (Online) http://www.fas.org/irp/program/dsb_battlefield_rep.htm.

Denning, D.E. (1999): *Information Warfare and Security*. ACM Press, New York, NY, 1999.

Drucker, P.F. (1995): *Managing in a Time of Great Change*. Truman Talley, New York, 1995.

Federation of American Scientists [FAS] (1996): *The Intelligence Cycle*. 1996. (Online) http://www.fas.org/irp/cia/product/factell/intelcycle.htm.

Federation of American Scientists [FAS] (2002): *Nuclear Forces Guide*. (Online) http://www.fas.org/nuke/guide/index.html.

Galbraith, J.R. and Kazanijan, R.K. (1986): *Strategy Implementation*: *Structure, Systems and Processes*. 2nd ed., West, St. Paul, MN, 1986.

Gannon, J.C. (2000/1): *Analytical Uses of Collaboration*. 2000. (Online) http://www.cryptome.org./cia_auc.htm.

Gannon, J.C. (2000/2): *Intelligence Challenges Trough 2015.* (Online) http://www.odci.gov/cia/public_affairs/speeches/gannon_speech_05022000.html.

Gartner Group (1998): *Knowledge Management Scenario*. *C*onference presentation, 1998.

Grant, R.M. (2002): *Contemporary Strategy Analysis*. 4th ed., Blackwell, Malden, MA, 2002

Grossman, M. (2002): *Seven Themes that Shape our World*. U.S. Department of State, International Information Programs, March 1, 2002. (Online) http://usinfo.state.gov/topical/pol/nato/02032705.htm.

Grudin, J. (1996): *Evaluating Opportunities for Design Capture*. in: T. P. Moran and J. M. Carroll (Eds.): *Design Rationale: Concepts, Techniques and Use*. Lawrence Erlbaum Associates, Mahwah, NJ, 1996.

Hořejší, T. (1997): *Bezpečnost státu*: *Pozdní procitnutí*. (State Security: Late Awakening) Týden (Week), No. 50, December 8, 1997. in: Williams, K., Deletant, D. (2001): *Security Intelligence Services in New Democracies. The Czech Republic, Slovakia and Romania,* p. 83. Palgrave, New York, N.Y., 2001.

Hutchins, E. (1991): *Organizing Work by Adaptation*. Organization Science 2(1), 1991.

IC21: *The Intelligence Community in the 21st Century*. (2000) Permanent Select Committee On Intelligence, House of Representatives. Staff study. U.S. Government Printing Office, 2000. (Online) http://frwebgate5.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=667669372

Jane's Intelligence Review (2000): *Managing Information Overload*. March, 2000. (Online) http://jir.janes.com.

Jansen, W., Steenbakkers, G.C.A., and Jägers, H.P.M. (2000): *Knowledge Management and Organization Design*. in: Malhotra, Y. (ed., 2000): *Knowledge Management and Virtual Organizations*. Idea Group Publishing, Hershey, PA, 2000.

Johnson, S.E. and Libicki, M. C. (1996): *Dominant Battlespace Knowledge.* National Defense University Press, Washington D.C., 1996.

Joint Staff Publication No. 1-02 [JP-1.02.] (1994): *Department of Defense Dictionary of Military and Associated Terms*. in: US Federal Standard 1037-C: *Telecommunications: Glossary of Telecommunication Terms*. 2000 (Online) http://www.its.bldrdoc.gov/fs-1037/dir-010/_1401.htm.

Lave, J. (1988): *Cognition in Practice: Mind, Mathematics, and Culture in Everyday Life*. Cambridge University Press, 1988.

Lave, J. and Wenger, E. (1990): *Situated Learning: Legitimate Peripheral Participation*. Cambridge University Press, 1990.

Lefebvre, S. (1995): *The Army of the Czech Republic: A Status Report.* Journal of Slavic Military Studies, Vol. 8, Is. 4., December 1995.

Levitt, B. and March, J. (1988). *Organizational Learning*. Annual Review of Sociology, pp. 319-340, Vol. 14, 1988.

Liebowitz, J. (ed., 1999): *Knowledge Management Handbook*. CRC Press, Washington, D.C., 1999.

Lowenthal, M.M. (2000): *Intelligence*. *From Secrets to Policy.* CQ Press, Washington, D.C., 2000.

Malhotra, Y. (2000): K*nowledge Management and New Organizational Forms*: *A Framework for Business Model Innovation*. in: Malhotra, Y. (ed., 2000): *Knowledge Management and Virtual Organizations*. Idea Group Publishing, Hershey, PA, 2000.

Marenches, A. and Andelman, D.A.(1992): *The Fourth World War: Diplomacy and Espionage in the Age of Terrorism*. New York: William Morrow, 1992

Martin, F.T. (1998): *Top Secret Intranet*. Prentice Hall, Upper Saddle River, NJ, 1998.

Michta, A.A. (ed., 1999): *America's New Allies. Poland, Hungary, and the Czech Republic in NATO*. University of Washington Press, Seattle and London, 1999.

Miller, J.H. (1995): *Information Warfare: Issues and Perspectives.* March, 1995. (Online) http://www.inss.com
Lefebvre, S.: *The Army of the Czech Republic: A Status Report.* Journal of Slavic Military Studies, Vol. 8, Is. 4., December 1995.

Nastoupil, R. (1999): *Current Czech Defense Policy.* Journal of Slavic Military Studies, Vol. 12, Is. 2., Jun 1999.

National Security Strategy (2001). (Online)
http://www.vlada.cz/1250/vrk/rady/brs/dokumbrs/strategie2001.pdf.

National Military Strategy (1999). (Online)
http://www.vlada.cz/1250/vrk/rady/brs/dokumbrs/rok99/vojenstr.il2.htm.

NATO Open Source Intelligence Handbook [NOSINTH] (2001). U.S Army, 2001.

Nissen, M.E., Kamel, M., Sengupta, K. (2000): *Integrated Analysis and Design of Knowledge Systems and Processes*. Information Resources Management Journal, January-March 2000.

Nissen, M. (2001): *Facilitating Naval Knowledge Flow*. Naval Postgraduate School, NPS-GSBPP-01-004, 2001.

Nonaka, I. (1994): *A Dynamic Theory of Organizational Knowledge Creation*. Organizational Science Magazine, May 1994.

O'Hanlon, M.E. (2000): *Technological Change and the Future of Warfare.* The Brookings Institution, Washington D.C., 2000.

O'Leary, D.E. (1998): *Enterprise Knowledge Management*. Computer Magazine, March 1998.

Open Source Intelligence Handbook [OSINTH] (1997). Proceedings of the 6th International Conference *Global Security and Global Competitiveness: Open Source Solutions*. Open Source Solutions Inc., 1997.

Owens, W.A. (2000): *Lifting the Fog of War*. Farrar, Straus and Giroux, New York, 2000.

Oxendine, E. (2000): *Knowledge Management Support to Network-Centric Warfare (NCW)*. Master Thesis, Naval Postgraduate School, September 2000.

Oxendine, E. and Nissen, M.E. (2001): *Knowledge Process and System Design for the Carrier Battle Group*. Knowledge and Innovation: Journal of the Knowledge Management Consortium International. Vol. 1, No. 3, April 15, 2001.

Reform of the Armed Forces of the Czech Republic: *Objectives and Principles* (2001). Center for Preparation of the Armed Forces Reform, Prague. (Online) http://www.army.cz/reforma/english/dokument.htm.

Ruggles, R. (1997): *Knowledge Management Tools*. Butterworth-Heinemann, Boston, MA, 1997.

SANANIM—Drug Information Server. 2002 (Online) http://www.sananim.cz/dis/index.htm.

Schwartau, W. (1996): *Information Warfare*. 2nd ed. Thunder's Mouth Press, New York, 1996.

Steele, R.D. (1993): *Theory and Practice of Intelligence in the Age of Information*. Open Source Solutions, Inc., 1993. (Online) http://www.oss.net.

Suchman, L. (1987): *Plans and Situated Actions: the Problem of Human-Machine Communication*. Cambridge University Press, 1987.

Tenet, G.J. (2000): *The Worldwide Threat in 2000*. Washington, D.C., 2000. (Online) http://www.cia.gov/cia/public_affairs/dci_speech_020200.html.

Ulrych, M.P. (1999): *Democratizing Communist Militaries: The Cases of the Czech Republic and Russian Armed Forces.* Ann Arbor: University of Michigan Press, 1999.

Wagner, J.A., Hollenbeck, J.R. (1998): *Organizational Behavior*. 3rd ed. Prentice Hall, Upper Saddle River, NJ, 1998

Weber, M. (1968): *Economy and Society*: *An Outline of Interpretive Sociology*. University of California Press, Berkeley, 1968.

Wiig, K.M. (1999): *Introducing Knowledge Management into the Enterprise*. in: Liebowitz, J. (ed., 1999): *Knowledge Management Handbook*. CRC Press, Washington, D.C., 1999.

Williams, K., Deletant, D. (2001): *Security Intelligence Services in New Democracies. The Czech Republic, Slovakia and Romania.* Palgrave, New York, N.Y., 2001.

Zákon o zpravodajských službách č. 153/1994Sb. (Intelligence Services Act No. 153, 1994)

Zpráva o situaci v oblasti veřejného pořádku a vnitřní bezpečnosti na území České Republiky v roce 2000. (Report on the internal security in the Czech Republic in 2000) Ministry of Interior, 2001. (Online) http://www.mvcr.cz/dokumenty/bezp_si00/2_11krim.html.

Zuboff, S. (1988): *In the Age of the Smart Machine*. Basic Books, 1988.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
 Ft. Belvoir, Virginia

2. Dudley Knox Library
 Naval Postgraduate School
 Monterey, California

3. Dr. Mark E. Nissen
 Naval Postgraduate School
 Monterey, California

4. Kenneth R. Dombroski
 Naval Postgraduate School
 Monterey, California

5. Ministry of Defense
 General Staff
 J-2, Chief
 Kafkova 19 P.O.B 238
 160 41 Prague, Czech Republic



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A BURNING NEED TO KNOW: THE USE OF OPEN SOURCE INTELLIGENCE IN THE FIRE SERVICE

by

Thomas A. Robson

March 2009

Thesis Advisor:	Richard Bergin
Thesis Co-Advisor:	Robert Simeral

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2009	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE A Burning Need to Know: The Use of Open Source Intelligence in the Fire Service		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Thomas A. Robson			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

In the aftermath of September 11, 2001, the fire service found itself on the forefront of the war on terror. The people within the fire service began to realize they needed to share intelligence information with other government agencies in order to protect firefighters, and their community. At the federal level, the National Information Sharing Strategy recognized that first responders are critical to the prevention of terrorism and that an effective flow of intelligence information must be established between federal, state, local agencies.

Yet, the fire service has little experience in the field of intelligence and much of the intelligence available may not be specific or useful to the fire service. The local fire department is faced with the task of analyzing what a particular piece of information means to that department. Only the local department knows its procedures and locale well enough to accomplish this critical task.

This thesis seeks to assist local fire departments in building systems and training personnel to exploit open source intelligence for their unique needs. Using information gleaned from interviews with experienced intelligence people, the intelligence cycle is discussed including requirements, collection, analysis, and dissemination in light of the needs of the fire service.

14. SUBJECT TERMS Fire, Intelligence, Firefighter Training, First Responders, Fire Service Intelligence, Open Source Intelligence, Fire Service			**15. NUMBER OF PAGES** 97
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release distribution is unlimited

A BURNING NEED TO KNOW: THE USE OF OPEN SOURCE INTELLIGENCE IN THE FIRE SERVICE

Thomas A. Robson
Battalion Chief, Fire Department, City of New York
B.S., Brooklyn College, 1980
D.D.S., New York University, 1984
M.A., University of Balamand, 2003

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2009**

Author: Thomas A. Robson

Approved by: Richard Bergin
Thesis Advisor

Robert Simeral
Thesis Co-Advisor

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In the aftermath of September 11, 2001, the fire service found itself on the forefront of the war on terror. The people within the fire service began to realize they needed to share intelligence information with other government agencies in order to protect firefighters, and their community. At the federal level, the National Information Sharing Strategy recognized that first responders are critical to the prevention of terrorism and that an effective flow of intelligence information must be established between federal, state, local agencies.

Yet, the fire service has little experience in the field of intelligence and much of the intelligence available may not be specific or useful to the fire service. The local fire department is faced with the task of analyzing what a particular piece of information means to that department. Only the local department knows its procedures and locale well enough to accomplish this critical task.

This thesis seeks to assist local fire departments in building systems and training personnel to exploit open source intelligence for their unique needs. Using information gleaned from interviews with experienced intelligence people, the intelligence cycle is discussed including requirements, collection, analysis, and dissemination in light of the needs of the fire service.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
A. PROBLEM STATEMENT 1
B. RESEARCH QUESTION 3
C. LITERATURE REVIEW 3
1. History 3
2. Open Source Intelligence 4
3. Open Source Intelligence in Homeland Security 8
4. The Intelligence Cycle 10
D. ARGUMENT: MAIN CLAIMS, WARRANTS, EVIDENCE, AND CHALLENGES 13
E. SIGNIFICANCE OF THE RESEARCH 15

II. RESEARCH METHODOLOGY 17
A. INTERVIEW PROTOCOL 17
B. BIOGRAPHIES 19
1. Fred Burton 19
2. George Friedman 20
3. Mark Johnson 20
4. John McCreary 21
5. Patrick Miller 22
C. QUALITATIVE ANALYSIS 24
1. Coding and Analysis 24
2. Writing 28

III. DATA ANALYSIS 31
A. INTELLIGENCE 31
1. Purpose 31
2. Open Source Intelligence 33
3. The Intelligence Cycle 34
B. REQUIREMENTS 36
1. Brainstorming 36
2. Freedom 37
3. Guidelines 38
C. COLLECTION 42
1. External Sources 42
2. Internal Resources 47
D. ANALYSIS 52
1. Uncertainty 53
2. Team Approach 53
3. Operations 60
E. DISSEMINATION 63
1. Information Transfer 63
2. Feedback 65

IV. RECOMMENDATIONS 67
A. TRAINING 67
1. Formal Instruction 67
2. Mentoring 69
B. KEEPING IT REAL 70
V. CONCLUSIONS 73
A. PROPOSITIONAL MODEL 73
B. INTELLIGENCE IN THE FIRE SERVICE 74
LIST OF REFERENCES 77
INITIAL DISTRIBUTION LIST 81

LIST OF FIGURES

Figure 1. Emergent Analytical Codes and Categories 28
Figure 2. Stages of the Intelligence Cycle: Description and Representative Quotes 35
Figure 3. Propositional Model 74

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS

ACLU	American Civil Liberties Union
CIA	Central Intelligence Agency
DIA	Defense Intelligence Agency
DHS	U.S. Department of Homeland Security
DNI	Director of National Intelligence
EMT	Emergence Medical Technician
FBI	Federal Bureau of Investigation
FDNY	Fire Department, City of New York
FDSOA	Fire Department Safety Officers Association
FOUO	For Official Use Only
FSIE	Fire Service Intelligence Enterprise
IED	Improvised explosive device
NYPD	New York City Police Department
OI&A	DHS Office of Intelligence and Analysis
OSAC	Overseas Advisory Council
OSC	U.S. Open Source Center
OSINT	Open source intelligence
PSA	Protective Security Advisor
SME	Subject matter expert
Stratfor	Strategic Forecasting, Inc.
SWAT	Special Weapons and Tactics
TLO	Terrorist Liaison Officer
USCG	U.S. Coast Guard

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Before all I acknowledge Him who strengthens me.

I want to thank Joan for putting up with all of this. Thank you for all the love and support.

I would like to express my sincerest gratitude to Richard Bergin and Robert Simeral for their invaluable advice on this thesis.

I am also extremely grateful to Fred Burton, George Friedman, Mark Johnson, John McCreary, and Patrick Miller for taking time out of their busy lives to be interviewed by me.

In addition, I want to express my heartfelt thanks to Battalion Chief Frank Montagna for all of his assistance on this project.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

Traditionally, the fire service was not a consumer of open source intelligence, nor was the processing of counterterrorism intelligence considered a normal function of local fire departments. However, in the aftermath of the September 11, 2001 attacks, the fire service suddenly found itself on the front row of the war on terror with a need to receive vital intelligence. This need for supplying information to local governments, including local fire departments, was also recognized on the national level. Many federal documents, especially Executive Order 13356, seek to strengthen the sharing of counterterrorism intelligence between federal entities and local governments. Further, the National Information Sharing Strategy recognizes that first responders are critical to the prevention of terrorism and that an effective and efficient flow of intelligence information must be established between federal, state, local, and tribal authorities.[1] Additionally, some fire departments such as the Fire Department of the City of New York (FDNY) seek to establish efficient information transfer arrangements between it and other governmental entities.[2] The ultimate goal of this intelligence sharing effort is the prevention or mitigation of terrorist attacks on the United States and the local community.

"Open Source Intelligence or OSINT is unclassified information that has been deliberately discovered, discriminated, distilled, and disseminated to a select audience in order to address a specific question."[3] For the fire service, the specific question to be answered is how is what is happening in the field of terrorism going to affect its operations, the safety of its personnel, and the safety

[1] *National Strategy for Information Sharing* (Washington, D.C.: The White House, October 2007), 3.

[2] *Terrorism and Disaster Preparedness Strategy* (New York: Fire Department of the City of New York 2007), 20.

[3] *NATO Open Source Intelligence Handbook* (North Atlantic Treaty Organization, November 2001), v.

of the people they serve. For instance, information available on a jihadi website might show an increase in the use of secondary devices during jihadi attacks. When discovered and disseminated to fire department units this intelligence may save the lives of firefighters and the citizens they are sworn to protect. Currently, the fire service is not guaranteed access to this information or it is subject to such a large flow of information that this critical nugget of intelligence may be overlooked.

Additionally, since most fire department personnel do not have security clearances, the most useful type of intelligence information is open source intelligence (OSINT), especially since most fire departments will want to disseminate intelligence information to all of its members. "Due to its unclassified nature, OSINT can be shared extensively without compromising national security."[4] The difficulty encountered with the reception of open source intelligence is that the fire service is generally not currently equipped to handle it. Assuming the local fire department is receiving intelligence, the flow of information coming out of the Federal government and local fusion centers is massive and requires additional processing by fire departments to exploit this intelligence properly. Additionally, much of the information flow may not be specific or useful to the fire service. Much of it tends to be for use by the law enforcement community. Therefore, though the fire service may receive large amounts of open source information, it will not necessarily obtain a large amount of OSINT for most of the information received will be valueless. Hence, the local fire department needs to separate out what it finds useful from this information flow. This is called the signal-to-noise problem. Therefore, local fire departments need specifically trained personnel and systems to accomplish this processing and analysis. Most fire departments do not have the systems or the personnel in place to exploit this information flow, nor do they have the

[4] Eliot Jardines, *Using Open Source Information Effectively: Hearing Before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security of the House of Representatives June 21, 2005* (Washington, D.C.: U.S. Government Printing Office, 2007), 13.

experience to build such systems. The proposed thesis will research the building of processes, and systems to obtain, process, and evaluate open source intelligence efficiently for use by the fire service.

B. RESEARCH QUESTION

How could local fire departments build systems and train personnel to exploit open source intelligence for their unique needs?

C. LITERATURE REVIEW

1. History

Since the fire service is a new player in the intelligence field, there is little written about its role or its usage of intelligence. However, the first fire department formally to look at the use of intelligence to support its operations was the Fire Department of the City of New York (FDNY). After the September 11, 2001 attacks, the FDNY realized it needed situational awareness and intelligence on terrorism to prepare, respond, and recover better from a possible attack. The FDNY formalized its vision in its 2007 document *Terrorism and Disaster Preparedness Strategy*. The strategy states, "Terrorists have proved they are extremely adaptive and reactive to changes in the security environment. Therefore, to be truly prepared for terrorist incidents the Department must be adaptive to new threats . . ."[5] To this end, the FDNY began to meet with the Department of Homeland Security in order to discuss information and intelligence sharing. "The Department of Homeland Security's Office of Intelligence and Analysis (OI&A) and the Fire Department of the City of New York (FDNY) met in New York in fall of 2006 to discuss fire service writ large as partners in sharing homeland security information. Both agencies agreed about the vital need to share information for the security of the Nation against enemies' hostile

[5] *Terrorism and Disaster Preparedness Strategy* (New York: Fire Department, City of New York, 2007), 10.

intentions (counterterrorism information)."[6] Additionally, both agencies agreed that other fire departments should be brought into the Fire Service Intelligence Enterprise in order to share information horizontally as well as vertically. In addition, if fire departments kept each other informed of what is occurring in their locality, seemingly isolated incidents may show a pattern that indicates terrorist activity. To that end, fifteen major city fire departments have agreed to form a trusted network, a "community of interest" to share intelligence and lessons learned.[7]

Several theses have recently come out of the Naval Postgraduate School discussing various aspects of intelligence in the fire service. Much of the emphasis has been on the role of the firefighter as an intelligence collector. Additionally, the Center for Policing Terrorism released a report recommending the fire service "serve a preventive intelligence role."[8] Other theses have recognized the need for the fire service to move from a reactive to a proactive posture by the use of intelligence in planning and training.

2. Open Source Intelligence

Open source intelligence or OSINT seeks to analyze information found in television broadcasts, radio broadcasts, newspapers, the internet, academic and scientific journal articles, commercial data, non-secret foreign governmental reports, and speeches by foreign politicians. OSINT, by definition, is not collected by illicit means. The advantage to using open source intelligence to the American fire service is that most of its members do not have security clearances. OSINT may be widely distributed within a department with only an "sensitive but unclassified" or a "for official use only" caveat. Some agencies use an additional caveat "law enforcement sensitive" for certain specialized materials

[6] Fire Service Intelligence Enterprise (FSIE)*: Progress Report 1*, (U//FOUO) (December 28, 2007), 2.

[7] Ibid., 4.

[8] Kyle Dabruzzi and Daveed Gartenstein-Ross, "Firefighters' Developing Role in Counter Terrorism," *Policing Terrorism Report* 3 (July 2008), 5.

that demand additional dissemination restrictions; however, the distinctions within the field of "sensitive but unclassified" materials are somewhat artificial. Intelligence marked "secret" and "top secret" may be advantageous to the highest levels of a department; however, it will never allow situational awareness for the rest of a department unless it can be "sanitized" to unclassified. OSINT may also inform higher echelons of a fire department about what information they are lacking, allowing them to go to the federal government for additional information or clarification.

What is the value of OSINT? The literature shows that for many traditional analysts, open source information was a starting point in the collection or analysis of other forms of intelligence. OSINT is thought to create a background for the analyst to help him or her understand the issues and people involved in a particular matter. However, OSINT can also be used to verify or supplement other intelligence sources.[9] Additionally, foreign newspapers and speeches made by a terrorist organization's higher-level leadership may give a window into the collective mind of these groups. Speeches and articles written by foreign policy makers may also provide insight into their hopes and concerns as well. It may be useful in the evaluation of societal and economic trends. It may be used to track dual-source technology that could be used in the production of WMDs and its supply network. Yet another benefit to OSINT is that since it is derived from open sources, it may be possible to release the intelligence to foreign leaders or the press if beneficial to the United States without revealing its classified sources and methods.

There is another area of OSINT sources called "gray literature." Gray literature consists of limited availability materials where there are few copies produced. Alternatively, the existence of this type of literature may be for the most part unknown or has a restricted distribution through specific channels. These materials may consist of "working papers, pre-prints, technical reports and

[9] *Open Source Intelligence*, (U//FOUO) (Washington, D.C., Department of the Army, December 5, 2006), 2-2.

technical standards documents, dissertations, data sets, and commercial imagery," internal use only documents and articles, journals, and reports prepared for specific organizations or associations.[10] This literature is, by its very nature, difficult to search for and acquire; for instance, some trade literature available at a show and papers delivered at a conferences may only be distributed to those at the trade show or conference.[11]

OSINT has several limitations. One is that an analyst will rarely find information that foreign governments are trying to hide in open sources. In other words, you will not generally find secrets there. OSINT will, therefore, rarely supply the "'smoking gun' about some issue or threat."[12] Consequently, OSINT may not be a replacement for other forms of intelligence. It relies on information that is fragmentary and open to various interpretations. This means OSINT must be fit into the larger picture. Due to the volume of the data flow, policy makers must understand that the OSINT analyst may completely miss important information.

As was mentioned previously, one of the problems with creating OSINT is that the amount of raw information available is voluminous and even with sophisticated software, it still requires many resources to translate, cull, and convert it into a form that can be useful in generating intelligence. OSINT analysts will look for a wide range of information, ideally, from many different types of open sources in an effort to confirm a possible piece of intelligence. However, having a large amount of open source information will not necessarily give you a large amount of OSINT for most of the information received will be

[10] *NATO Open Source Intelligence Handbook* (North Atlantic Treaty Organization, November 2001), 8.

[11] *NATO Open Source Intelligence Reader* (North Atlantic Treaty Organization, February 2002), 25.

[12] Jennifer Sims and Burton Gerber, eds., *Transforming U.S. Intelligence* (Washington, D.C.: Georgetown University Press, 2005), 67.

valueless (the signal-to-noise problem or "wheat and chaff problem").[13] The rest must be "filtered" and, ideally, verified before it can be passed on to other analysts, department policy makers, or personnel.

An additional problem with OSINT is that, though there can be a collection strategy, the analyst has no ability to task its collection as can be done with the other "INTs." For example, the analyst cannot control what foreign newspapers will print, or what speeches terrorist groups will make, which means the information the OSINT analyst needs may or may not be available when he or she needs it. The analyst must, instead, sit by their stream of information and see what type of fish they hook. This leads to a further complication, since the analyst has no control over its production, they must be careful in the intelligence vetting process because the open source information received may be disinformation or propaganda placed there by foreign governments. However, for every major or minor event in the world, at least 20 independent sources report on the very same event.

The risk and possibility of misinformation or deception have grown, but the risk also has been reduced. It has become harder for remote and closed areas of the world to keep things secret and to fool its own citizens with propaganda.[14] Additionally, since open source information is available to everybody, there will be pressure to release some analysis before, for instance, the *New York Times* does. However, the OSINT analyst must not rush this vetting process, or the risk of creating incorrect intelligence increases.

[13] Mark M. Lowenthal, *Intelligence: From Secrets to Policy,* 3rd ed. (Washington, D.C.: CQ Press, 2006), 102.

[14] *NATO Open Source Intelligence Reader* (North Atlantic Treaty Organization, February 2002), 80.

3. Open Source Intelligence in Homeland Security

"In today's complex and dangerous world, US policy makers need contextual, contemporary, and relevant knowledge to make decisions."[15] This is most certainly true of the leadership of the fire service in the United States. In the effort to protect the homeland, whether from natural disasters or from terrorist attack, firefighters will be sent into harm's way. Their departments and the national government owe them the best training, information, and equipment available. Training firefighters to respond to terrorist incidents can only be done if the leadership of a department has information at hand to plan and execute training properly. The same is true for the types of equipment a department might purchase. Similarly, current situational awareness is critical to the safety of firefighters. Awareness of an impending attack could lead to an increase of staffing or changes in firefighting procedures and response patterns. Firefighting is an inherently dangerous occupation; no amount of information can eliminate those risks. However, intelligence about the current terrorism landscape and its future possibilities can reduce those risks to the extent possible.

In his testimony before the U.S. Congress on the value of OSINT in the realm of homeland security, Eliot A. Jardines stated, "From Pearl Harbor to the September 11th terrorist attacks, intelligence failures have largely resulted not from a lack of information, but rather the inability to effectively disseminate that information or intelligence."[16] Others posit, "major intelligence failures are usually caused by failures of analysis."[17] He also points out that the use of OSINT effectively bypasses the problem of obtaining security clearances for each first responder. "In fact, OSINT products could be disseminated to the full complement of first responders such as firefighters, EMTs, university police

[15] Eliot A. Jardines, *National Open Source Enterprise* (Washington, D.C.: Office of the Director of National Intelligence, April 2006), 6.

[16] House Subcommittee on Intelligence, information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security, *Using Open Source Intelligence Effectively*, 109th Cong., 1st sess., 2005, 13.

[17] Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, D.C.: Center for the Study of Intelligence, 1999), 65.

departments, hospitals, and private security firms. Consider for a moment what a paradigm shift that would represent."[18] It is important to note here that a fire department analyzing its own needs and requirements and attempting to fulfill those requirements does not mean cutting itself off from other sources of information such as federal and state governments. For instance, Charles Allen reported, "DHS Intelligence is developing a strong Open Source Intelligence (OSINT) capability focused on our areas of expertise and responsibility to complement the broader Intelligence Community's open source investments."[19] Fire departments will continue to be dependent on these sources as well. Indeed, fire departments developing products for their internal use may want to release them through DHS because they may be of real interest to other members of the fire service.

The testimony before the committee also made it clear that open source intelligence is not a panacea nor can it be separated from other sources of intelligence.[20] However, it is the best way to ensure homeland security intelligence is as widely distributed as possible. Wide distribution ensures that homeland security intelligence is in the hands of the people who can tactically use it. A United States Navy Air Wing Commander leading the first flights over Baghdad said, "If it is 85% accurate, on time, and I can share it, this is a lot more useful to me than a compendium of Top Secret Codeword material that is too much, too late and needs a safe and three security officers to move it around."[21] This is true for homeland security intelligence as well. Produced materials should be kept at a "For Official Use Only" level to ensure some level of security. In addition, individual fire departments need to be able to use open source materials without violating an individual's Constitutional rights.

[18] House, Committee, *Using Open Source Intelligence Effectively*, 14.

[19] Senate Select Committee on Intelligence, *Intelligence Reform, and Homeland Security Intelligence*, 110th Cong. 1st sess., 2007, 4.

[20] House Committee, *Using Open Source Intelligence Effectively*, 4.

[21] Robert David Steele, *Open Source Intelligence: Executive Overview* (Global Intelligence Partnership Network, January 1, 2004), 21, http://www.oss.net/ (accessed April 18, 2008).

4. The Intelligence Cycle

The literature shows that proper intelligence, including open source intelligence, is an iterative process. The various steps in the intelligence process are distinct, but inseparable, if good intelligence products are to be delivered. This progression is called the intelligence cycle. There are several models of the intelligence cycle, however, all the models really involve the same concepts. For instance, even within the U.S. Army, there are different models in the literature. The model that appears in the U.S. Army's *Open Source Intelligence* manual describes a five-step model for the exploitation of open source intelligence. The five steps in this model are planning, preparing, collecting, processing, and production.[22] The U.S. Army Intelligence Center's guide, *Targeting Tomorrow's Terrorist Today*, describes five steps beginning with Planning and Direction. At this step, the possible sources of OSINT information is identified. Then comes the Collection phase in which the actual data is captured. The data is then run through the Processing, Integration, and Guidance phase. Then, hopefully, validated intelligence is analyzed and intelligence products produced in the Analysis and Production phase. Finally, the product reaches the Dissemination phase. At this phase, the level of restriction is decided since finished products may divulge OSINT collection capabilities.[23]

The United States Department of Justice's Bureau of Justice Assistance describes a six step cyclical process.[24] These steps consist of "Planning and Direction," in which this step leads to the actual Collection phase; for law enforcement, this is the most labor-intensive aspect of the intelligence

[22] *Open Source Intelligence*, *FMI 2-22.9* (U//FOUO) (Washington, D.C., Department of the Army, December 5, 2006), 3-1.

[23] Ben Benavides, *Targeting Tomorrow's Terrorist Today (T^4) through Open Source Intelligence (OSINT): Quick-Links Started Handbook for the Open Source Analyst*, (U//FOUO) (Fort Huachuca: U.S. Army Intelligence Center, January 2007), 48.

[24] *The National Criminal Intelligence Plan* (Washington, D.C.: US Department of Justice, June 2005), 3, http://www.it.ojp.gov/documents/National_Criminal_Intelligence_Sharing_Plan.pdf (accessed July 10, 2008).

process."[25] The information goes through a Processing/Collation phase. The results of that phase are put through an Analysis phase. Of course, analysis for law enforcement may be very different from either a national intelligence organization or a fire department. Police analysis should produce intelligence that gives leads in an investigation or results in prosecution, in addition to preparation for and prevention of terrorist attacks.[26] The product is then disseminated to those within the organization who need to know it. Reevaluation of the intelligence is then carried out resulting in a new period of planning and direction.

Other authors such as Lowenthal propose a seven-step intelligence process.[27] The first step in the seven-step process is identifying requirements. Requirements are the items that the open source process is supposed to clarify or on which to capture information. Within the Fire Service Intelligence Enterprise (FSIE), there is a Requirements Working Group, which is beginning to identify the requirements of the fire service. These fall into five broad categories. The first category of requirements is potential incidents and threats. The second requirement was time estimates as these can directly impact situational awareness and operational readiness.[28] Third, what are the general protective measures being taken by other agencies and levels of government.[29] The fourth requirement is such information that "informs fire service actions" such as protecting firefighters, their families, operations, and mission.[30] The last

[25] *Intelligence-Led Policing: The New Intelligence Architecture* (Washington, D.C.: US Department of Justice, September 2005), 6, http://www.ncjrs.gov/pdff.lesl/bja/210681.pdf (accessed July 7, 2008).

[26] Ibid.

[27] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 3rd ed. (Washington, D.C.: CQ Press, 2006), 102.

[28] Fire Service Intelligence Enterprise (FSIE)*: Progress Report 1*, (U//FOUO) (December 28, 2007), I-2.

[29] Ibid., I-3.

[30] Ibid.

requirements set identified was information on special events, target hazard analysis, natural disaster vulnerability and prediction, and cyber threats.[31]

This effort by the Fire Service Intelligence Enterprise to identify the common requirements of the fire service was necessary because homeland security intelligence is dominated by law enforcement, while the needs of the fire service may be quite different. "Several SMEs (subject matter experts) cited the overall lack of inclusion of these other disciplines (public health, fire, emergency medical services, and private sector security) at all levels as a critical shortcoming in the development of comprehensive, effective information and intelligence sharing processes."[32]

The next identified step in the intelligence cycle is collection. Collection is how the necessary information to fulfill the identified intelligence requirement is obtained. It is important to note that all that is being collected here is information, raw data if you will; this information is of little value until it is processed and analyzed. Requirements should give those tasked with producing the necessary intelligence as sense of how critical that particular requirement is. This allows the organization and the individual analyst to assign a priority to its collection. Without such information, critical requests may be delayed because the analyst is attempting to fulfill a request for intelligence that has little or lesser criticality.

The following step, Processing, seeks to eliminate superfluous and incorrect material and to arrange the data in a logical format.[33] In other words, the information is vetted and organized. Only then can an analyst begin to attempt to create a coherent picture out of the available information. This is where information and data become intelligence. Intelligence can be considered

[31] Fire Service Intelligence Enterprise (FSIE)*: Progress Report 1*, (U//FOUO) (December 28, 2007), I-3-4.

[32] U.S. Department of Homeland Security Lessons Learned Information Sharing, *LLIS Intelligence and Information Sharing Initiative: Homeland Security Intelligence Requirements Process* (December 2005), 4.

[33] *Intelligence-Led Policing: The New Intelligence Architecture* (Washington, D.C.: US Department of Justice, September 2005), 7, http://www.ncjrs.gov/pdff.lesl/bja/210681.pdf (accessed July 7, 2008).

a "concisely tailored answer reflecting a deliberate process of discovery, discrimination, distillation, and delivery of data precisely suited to need."[34] In other words, intelligence is an answer to a question asked by a policy maker, which draws upon known data and information, but put through a refinement process that adds value to existing information by the input of the analyst. The next part of the intelligence cycle is Dissemination; here, the finished product is moved to the people who requested it or can use the material. For instance, some product may be produced for the higher echelons of an organization for long-term planning and materials acquisition. This would be strategic intelligence. Other intelligence may be for day-to-day situational awareness. This is an example of tactical intelligence.

The sixth step, Consumption is important as well. Consumption means that the people who were supposed to read the prepared and disseminated intelligence actually read it. Finally, the people who read the intelligence respond to it. In an ideal world, they let the people who prepared the intelligence know, "what has been useful, what has not, which areas need continuing or increased emphasis, which can be reduced and so on."[35] Additionally, the intelligence product may raise additional questions in the consumer's mind, which, in turn, may lead to further requests for intelligence. These new requirements start the intelligence cycle again.

D. ARGUMENT: MAIN CLAIMS, WARRANTS, EVIDENCE, AND CHALLENGES

September 11, 2001 changed the world in many ways. Agencies, such as the local fire department, that had never considered themselves targets of terrorist attacks, now found themselves on the front line of defending their country and their community against terrorist attacks. This was new and

[34] Robert David Steele, *Open Source Intelligence: Executive Overview* (Global Intelligence Partnership Network, January 1, 2004), 3, http://www.oss.net/ (accessed April 18, 2008).

[35] Mark M. Lowenthal, *Intelligence: From Secrets to Policy,* 3rd ed. (Washington, D.C.: CQ Press, 2006), 64.

uncharted territory to the fire service. The ability of the fire service to execute its sworn duty to protect life and property in the local community, as well as, to the extent possible, protect the firefighters who serve there from the consequences of terrorism, is dependent on the efficient usage of intelligence. The fire service requires homeland security intelligence for everything from planning to response and mitigation. Fire departments, out in the community on building inspections or responding to routine emergencies, may be able to prevent terrorism with good intelligence that leads to situational awareness. Currently, most fire departments have no systems in place for effectively collecting, analyzing, and dissemination open source intelligence for their own use. Developing a system wherein fire departments can properly exploit useful open source intelligence would enhance firefighter safety and add to their ability to prevent terrorism in their community and more efficiently respond to and mitigate such an attack if it occurred.

Some might argue that having an in-house system in the local fire department to exploit open source intelligence is wasteful or unnecessary or both as counter-terrorism intelligence may be supplied by the Department of Homeland Security's Office of Intelligence and Analysis or by their local police department or by their regional fusion center. Evidence will show that while these flows of information are not to be ignored, they are primarily law enforcement oriented and not necessarily useful to a local fire department. In addition, the flow of intelligence from the above-mentioned agencies must still be further analyzed to discover what is most applicable to the local fire department. The needs of the fire service are different from other agencies. Others might posit that the Fire Service Intelligence Enterprise (FSIE) will solve a local departments intelligence needs. The FSIE is certainly a step in the right direction; however, this system still does not address the needs of the fire department in its local community. An additional alternative might be to place fire service personnel in the local fusion center. However, in some areas where a local fusion center per se does not exist and given the uneven quality and intent of local fusion centers, this may not be a viable alternative.

E. SIGNIFICANCE OF THE RESEARCH

The immediate consumers of this research will be fire departments and other government agencies that are non-traditional consumers of open source intelligence such as public health entities. The research will lay out a "game plan" by which fire departments can effectively develop, disseminate, and employ open source intelligence to support prevention, planning, and operations in the post 9-11 environment. The research will also be useful to government agencies that might be tasked with supporting the fire service with homeland security orientated intelligence. Homeland security practitioners will gain insight into setting up an effective system for the collection and use of OSINT in agencies outside the intelligence and law enforcement communities. Finally, private entities, such as hospitals, and utilities, may find this research valuable in creating intelligence systems useful with a view to protecting their facilities from a terrorist attack or dealing with the after effects of such an attack.

THIS PAGE INTENTIONALLY LEFT BLANK

II. RESEARCH METHODOLOGY

This thesis will study the use of intelligence in the fire service from a qualitative research approach. The study will use qualitative interviews focused on understanding processes and building the frameworks required for a fire department to use intelligence in order to protect life and property in the community they serve. This is what is referred to in the literature as "topical interviews."[36] What is most import here is for the researcher to find subject matter experts of sufficient experience as to be able to shed light on a particular problem or issue. In this particular case, little research has been done on the problem of intelligence use by the fire service, so the researcher must interview experts in other field of intelligence and apply the knowledge gained to a fire department intelligence unit.

A. INTERVIEW PROTOCOL

The problem of intelligence use by the fire service was studied by qualitative analysis because the field is not well researched, which means it is difficult to "generate hypotheses and develop quantitative measures."[37] To this end, five interviews of approximately one hour each were conducted with subject matter experts (SMEs) in the field of intelligence. Each SME had a minimum of fifteen years of experience in the intelligence field. Indeed, the average length of experience with intelligence is over 20 years. Interviewees were intentionally drawn from a wide range of intelligence backgrounds so that the problem of intelligence use in the fire service could be viewed from a variety of perspectives. Two interviewees serve with the federal government. One has a background in open source intelligence; the other has a forty-year background in military

[36] Herbert J. Rubin and Irene S. Rubin, *Qualitative Interviewing The Art of Hearing Data 2nd ed.* (Sage Publications, Thousand Oaks, CA, 2005), 11.

[37] Gail Fann Thomas, "Research Methods: Qualitative Data Analysis," 2, https://www.chds.us/courses/file.php/279/lecture_transcript/6-res_methods_qual_datas_analysis_transcript.doc?forcedownload=1 (accessed January 22, 2009).

intelligence. The third interviewee is a senior level chief in local law enforcement and has a thirty-three year background in police intelligence. Two have a background in private sector intelligence. The researcher conducted initial interviews between November 4, 2008 and November 25, 2008. The researcher personally performed all depth qualitative interviews. They were all conducted by telephone and recorded for accuracy. The interviews were later professionally transcribed into a Word document format.

The interviews were started by using what Rubin and Rubin referred to as a "hypothetical example."[38] The question was, "If you suddenly found yourself tasked with the mission of starting a fire department intelligence unit from scratch, how would you go about it?" This question was designed to allow the interviewee to talk freely about their take on the issue of the research question. Additionally, broadly worded main questions were prepared as a framework to insure all concepts gleaned from the literature were covered and that each part of the topic was thoroughly explored.[39] These follow-up questions were allowed to evolve as each prior interview was analyzed. This process of theoretical sampling was continued until all five interviews were completed. Theoretical sampling kept the interviewing process open to changes in direction as indicated by the data itself.[40] In addition to the main and follow-up questions, continuation probes were used to expand the depth of detail and elaboration probes were used to connect and further explore the themes and concepts covered by the main question. From the existing data, gaps were noted and follow-ups to the interviews were carried out via e-mail. Answers to follow-up interviews were received between November 26, 2008 and January 19, 2009.

[38] Herbert J. Rubin and Irene S. Rubin, *Qualitative Interviewing The Art of Hearing Data 2nd ed.*, (Sage Publications, Thousand Oaks, CA, 2005), 161.

[39] Ibid., 135.

[40] Juliet Corbin and Anselm Strauss, *Basics of Qualitative Research,* 3rd ed. (Sage Publications, Thousand Oaks, CA, 2008), 144.

B. BIOGRAPHIES

1. Fred Burton

Mr. Burton is one of the world's foremost authorities on security, terrorists, and terrorist organizations. In his capacity as Vice President for Counterterrorism and Corporate Security at Stratfor, Mr. Burton oversees the firm's terrorism intelligence service and consults with clients on security-related issues affecting their organizations or personal safety. He leads a team of terrorism experts and a global network of human intelligence sources to analyze and forecast the most significant events and trends related to terrorism and counterterrorism.

Mr. Burton is the author of *Ghost: Confessions of a Counterterrorism Agent*, a story of his role in the burgeoning terrorist threat in the 1980s and beyond.

Before joining Stratfor, Mr. Burton served as a special agent in counterterrorism for the U.S. Department of State, where he was involved with many high-profile operations. He orchestrated the arrest of Ramzi Yousef, mastermind of the first World Trade Center bombing, and investigated cases such as the assassination of Israeli Prime minister Yitzhak Rabin, the killing of Rabbi Meir Kahane, the al Qaeda New York City bombing plots before 9/11, and the Libyan-backed terrorist attacks against diplomats in Sanaa and Khartoum. He has also served as the U.S. liaison officer to several international security, intelligence, and law enforcement agencies, providing consulting on global intelligence and threat identification.

In addition, Mr. Burton has revolutionized the field of security by designing a unique and specialized protective program to safeguard CEOs, their families, employees, and physical facilities. His strategy is highly valued and has been implemented by governments and a number of the world's leading corporations.

2. George Friedman

Dr. Friedman is the founder and Chief Executive Officer of Stratfor (www.stratfor.com), a company he began in 1996 that is now a leader in private intelligence. Dr. Friedman guides Stratfor's strategic vision, helping shape the firm's long-range geopolitical forecasts as well as overseeing and tasking tactical intelligence operations.

Dr. Friedman is also the author of numerous articles and books on national security, warfare, and intelligence. His most recent book, *America's Secret War,* a *Barron's* Best Book of 2004, describes America's covert and overt efforts in the global war on terror. Dr. Friedman's next book, *The Next Hundred Years: a Forecast for the 21st Century*, is set for a January 2009 release.

Major television shows and radio programs such as CNN's *Lou Dobbs*, Fox News' *The O'Reilly Factor*, and NPR frequently invite Dr. Friedman to appear as a national security and international affairs intelligence expert. *Barron's* has cited Stratfor's analysis on numerous occasions and *Barron's* cover article featured an interview in October 2001. He has also been featured in *Time* magazine, *The New York Times* and the *Wall Street Journal* and quoted in reference to global issues in the *New York Times*, *USA Today*, *Fortune*, *International Herald Tribune* and many other domestic and international publications. Dr. Friedman has been the keynote speaker at numerous conferences and industry specific events for private organizations and government agencies.

Dr. Friedman received his bachelor's degree from the City College of the City University of New York and holds a Ph.D. in government from Cornell University.

3. Mark Johnson

Mr. Johnson is the Enterprise Partnership Manager for Homeland Security in the Open Source Center. In this role, Mr. Johnson interacts with homeland security related components of the federal, state, and local governments for the

U.S. Director of National Intelligence (DNI) Open Source Center (OSC). In this recently created position, Mr. Johnson seeks to facilitate relationships that will leverage all forms of openly available information to result in homeland security insights, actions, and impact. Open source intelligence includes: text, broadcast, video, data, geographic, and internet derived information. Open Source intelligence is a valuable source for analytical understanding, early warning, tip-offs, and event detection and tracking—especially topics with a foreign aspect impacting homeland security, such as terrorism, biological hazards, cyber threats, weapons of mass destruction, and narcotics trafficking.

Mr. Johnson is a professional geographer, intelligence officer, former U.S. Army officer, and senior manager whose 28-year federal career has centered on the use, collection, exploitation, and creation of open source information. Prior to his current assignment, Mr. Johnson directed the only center in the U.S. intelligence community focused solely on open source geospatial materials—the OSC Map Services Center. His assignments over the years have taken him from Bangor to Baghdad, Tucson to Tokyo and points in between. Mr. Johnson holds a Master of Information Systems from Virginia Tech and has frequently written, taught, and spoken on intelligence topics.

4. John McCreary

John F. McCreary is a distinguished 38-year veteran of defense intelligence. He is the author of the internationally acclaimed, nightly news commentary, NightWatch™. He has taught strategic analysis and warning to the intelligence staffs of 32 countries. He created and taught the U.S. National Warning Course from 1983 to 1992. Since October 1, 2008, he has served as the Highly Qualified Subject Matter Expert for Analysis Transformation for the United States Air Force Intelligence Analysis Agency.

Mr. McCreary has worked intelligence for both the U.S. Government and in private industry. From June 2006 to May 2008, Mr. McCreary was employed by dNovus RDI as Director of National Intelligence and Analysis and was

appointed Vice President for Intelligence Analysis in May 2007. He served the United States government from 1968 to May 2006 as an intelligence analyst with the Defense Intelligence Agency. From 1998 to May 2006, he served as Senior Level Expert for current intelligence and strategic warning, with the rank of SES/SL-4; senior intelligence advisor in the Joint Staff; senior intelligence analyst in the Defense Intelligence Agency. From 1993 to 1998, Mr. McCreary served as Senior Intelligence Officer for Asia, Directorate of Intelligence, J2, Joint Staff.

From 1998 to date, Mr. McCreary publishes *NightWatch*, an executive style, nightly analysis of significant international events with impact on U.S. national security. He has also written "The Latest Intelligence Crisis," with Richard A. Posner in *Intelligence and National Security*, Volume 23, in 2008, ***I**ntelligence as Evidence*, a J2 monograph published in 1996, *Analysis of Political Instability*, a J2 monograph published in 1995 and "Warning Cycles" in *Studies in Intelligence* in 1983.

Mr. McCreary has received multiple commendations, citations, medals, and awards from the Intelligence Community, the CIA, and the DIA. In 2004, he received a Presidential Rank Award for Meritorious Service, the only DIA analyst to ever have received this award. He graduated magna cum laude from the University of Illinois in 1968, majoring in Chinese and European history and graduated from Georgetown University Law Center, with the degree of Juris Doctor (JD) in 1975. He is also a member of the Georgetown University Law Journal.

5. Patrick Miller

Chief Miller has served thirty-three years with the Ventura California Police Department and currently serves as its chief. Chief Miller developed the Ventura Police Department's Intelligence-Led Policing Program and a County Terrorism Working Group. Over the years, Chief Miller has served the Ventura Police Department in a variety of ranks and roles, including Intelligence, SWAT,

Narcotics, and Field Task Forces. Additionally, Chief Miller has taught for over 25 years in the law enforcement field including Homeland Security, Leadership, Terrorism, Narcotics, Intelligence, and Criminal Law.

In addition, from 1986 to the present, Chief Miller has worked on special assignments for the Central Intelligence Agency. Chief Miller worked as a full-time case officer and on a contract basis on a variety of classified intelligence operations in Central and South America, including training, handling assets, preparing intelligence reports and briefs, and performing classified operational duties. He wrote or led policy development and implementation of U.S. Government counter-narcotics programs in Columbia and El Salvador in 1986 – 1988. Since 2001, Chief Miller has served on numerous panels and committees

Regarding terrorism, asymmetrical warfare, low-intensity conflict, insurgency, and threat assessment. Since 1993, he has been a guest lecturer at the CIA training facility at Camp Perry Virginia.

Chief Miller is on the editorial board of an internal CIA publication. He has been involved with authoring *Using Tactical Intelligence, Internal CIA Publication* in 1995, and *Protecting Your Community from Terrorism: Strategies for Local Law Enforcement* in 2005. He was also involved with authoring *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion*, and *Developing and Sharing Information and Intelligence in a New World: Fusion Center Guidelines*, also in 2005, and *A Law Enforcement Assistance and Partnership Strategy: Improving Information Sharing Between the Intelligence Community and State, Local, and Tribal Law Enforcement* in 2006.

Chief Miller received a Master's of Public Administration from Pepperdine University in 1980, completed the California Command College at the California Polytechnic University in 1996, and received a Master of Arts from the Naval Postgraduate School in Security Studies (Homeland Defense and Security) in 2005.

C. QUALITATIVE ANALYSIS

Qualitative analysis of these interviews used open coding hand-in-hand with axial coding.[41] Theoretical memos were also used. Making comparisons and asking "practical" questions to build theory were the major methods of analysis in this project.[42] Building sensitivity, defined by Corbin and Straus as "insight, being tuned in to, being able to pick up on relevant issues, events, and happenings in the data," were also an important part of the qualitative analysis process.

1. Coding and Analysis

A hybrid approach was taken in coding the interviews. This hybrid model is part way between a responsive interview formal coding schema and grounded theory models in that not every term was coded, but only concepts and themes that were closely related to the research question were selected.[43] The literature was reviewed in order to acquire understand of the themes and concepts that should be coded.[44] A grounded theory approach was used where the themes and concepts were allowed to emerge from the data. Line-by-line open coding, the breaking apart of data in order to generate additional concepts and themes that may not have appeared in the literature, was performed.[45] The researcher gathered data and analyzed it concurrently. This also allows the development of "sensitivity," whereby the researcher by "alternating processes of data collection

[41] Juliet Corbin and Anselm Strauss, *Basics of Qualitative Research*, 3rd ed. (Sage Publications, Thousand Oaks, CA, 2008), 198.

[42] Ibid., 72 - 73.

[43] Herbert J. Rubin and Irene S. Rubin, *Qualitative Interviewing The Art of Hearing Data*, 2nd ed. (Sage Publications, Thousand Oaks, CA, 2005), 223.

[44] Ibid., 221.

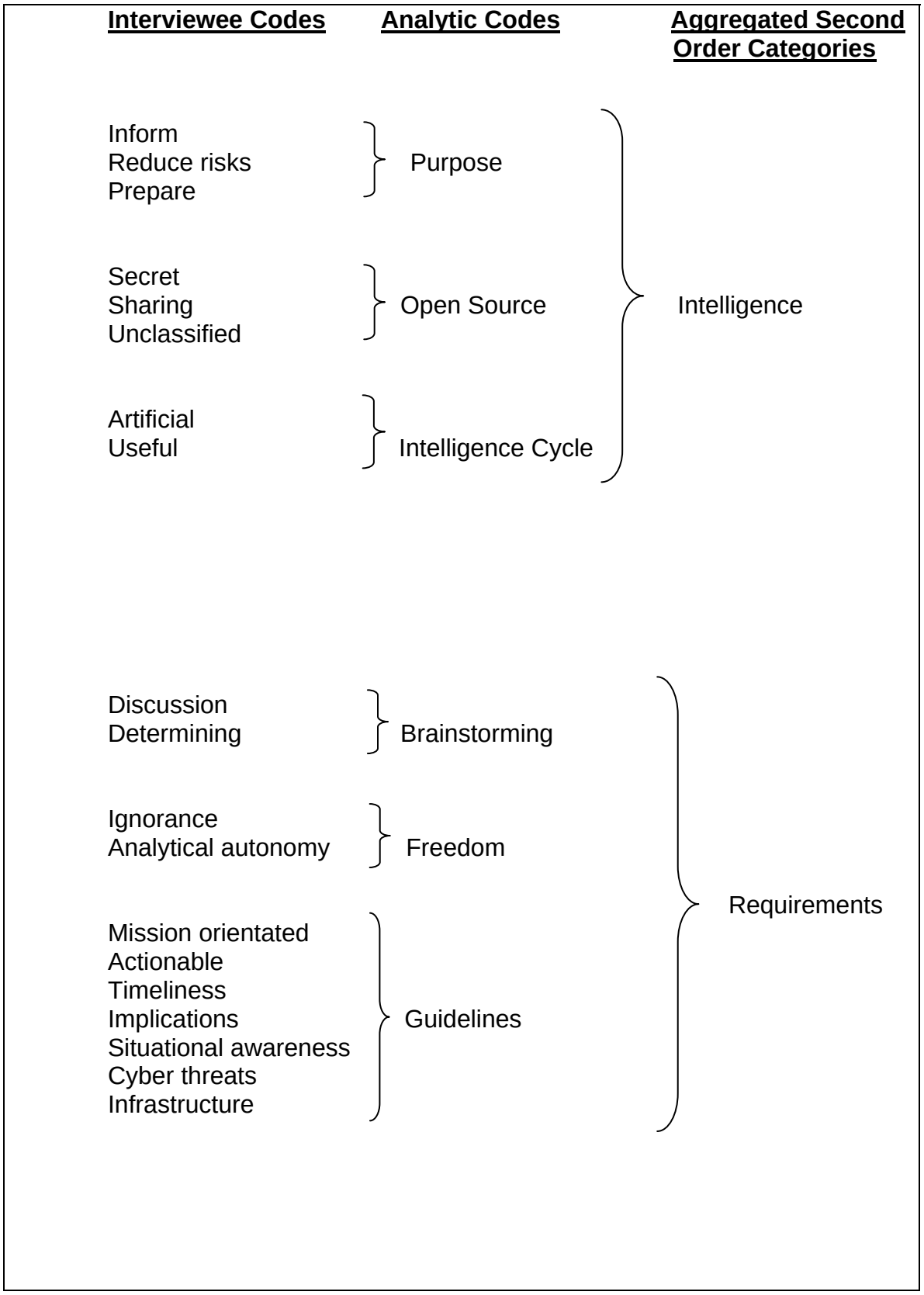
[45] Juliet Corbin and Anselm Strauss, *Basics of Qualitative Research*, 3rd ed. (Sage Publications, Thousand Oaks, CA, 2008), 198.

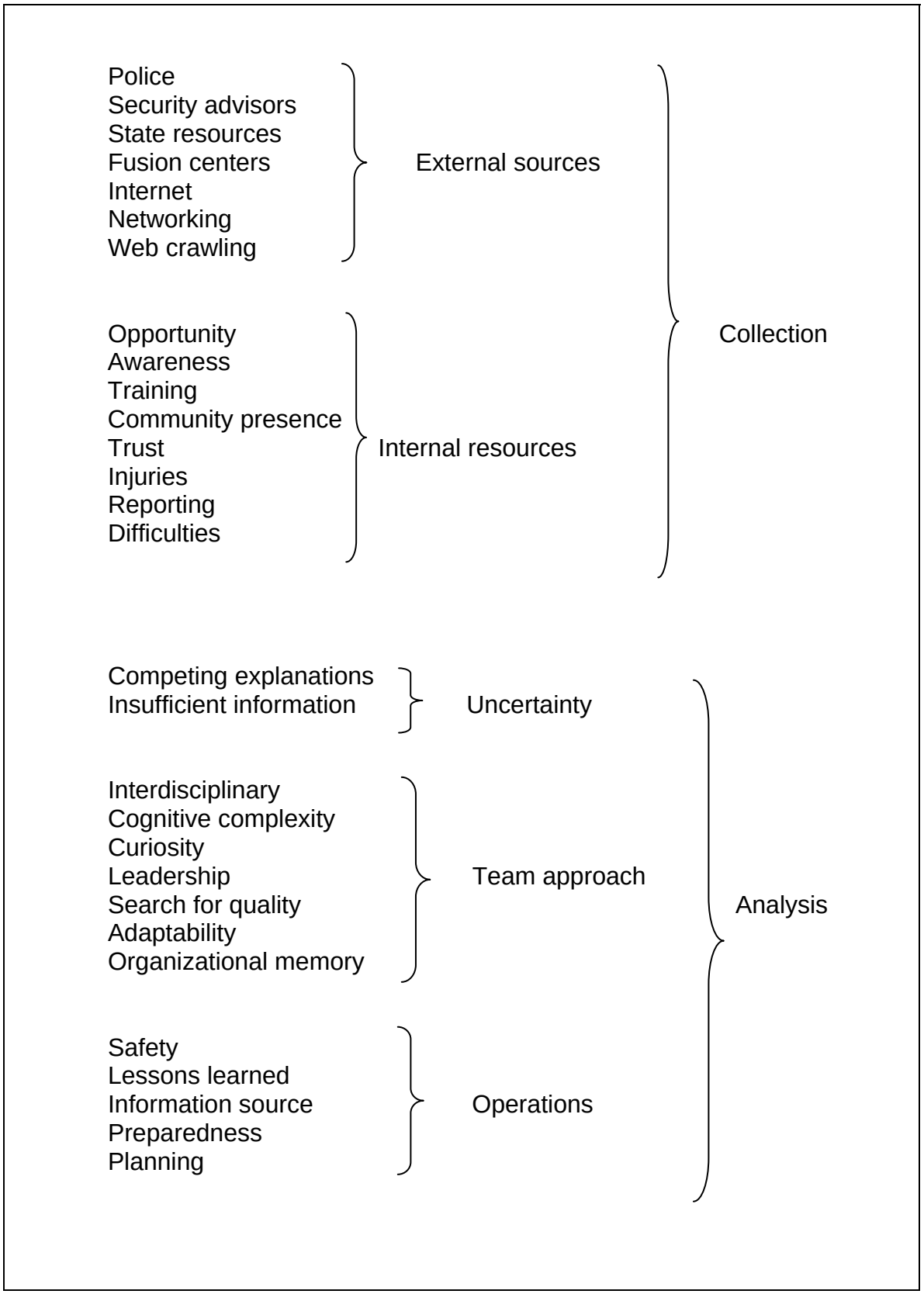
and analysis, meanings and significance of data, often illusive at first, becomes clearer and the researcher begins to see the issues and problems from the perspective of the participants."[46]

Data acquired from the interview transcripts, e-mails, and the researcher's field notes were coded and reviewed until coherent patterns began to emerge. This analysis was performed by "constant comparison." In this methodology, "incidents found to be conceptually similar are grouped together under a higher-level descriptive."[47] Constant comparison was necessary because it allowed the researcher to distinguish the various themes and concepts. Data was broken down into "informant codes," which were aggregated into higher order analytic codes and finally second order codes, and more general categories and themes, were induced (See Figure 1). Theoretical saturation was not reached due to time constraints mandated by the program.

[46] Juliet Corbin and Anselm Strauss, *Basics of Qualitative Research,* 3rd ed. (Sage Publications, Thousand Oaks, CA, 2008), 32.

[47] Ibid., 73.


Interviewee Codes
Analytic Codes
Aggregated Second Order Categories
Inform
Reduce risks
Prepare
Purpose
Secret
Sharing
Unclassified
Open Source
Artificial
Useful
Intelligence Cycle
Intelligence
Discussion
Determining
Brainstorming
Ignorance
Analytical autonomy
Freedom
Mission orientated
Actionable
Timeliness
Implications
Situational awareness
Cyber threats
Infrastructure
Guidelines
Requirements


Police
Security advisors
State resources
Fusion centers
Internet
Networking
Web crawling
External sources
Opportunity
Awareness
Training
Community presence
Trust
Injuries
Reporting
Difficulties
Internal resources
Collection
Competing explanations
Insufficient information
Uncertainty
Interdisciplinary
Cognitive complexity
Curiosity
Leadership
Search for quality
Adaptability
Organizational memory
Team approach
Safety
Lessons learned
Information source
Preparedness
Planning
Operations
Analysis

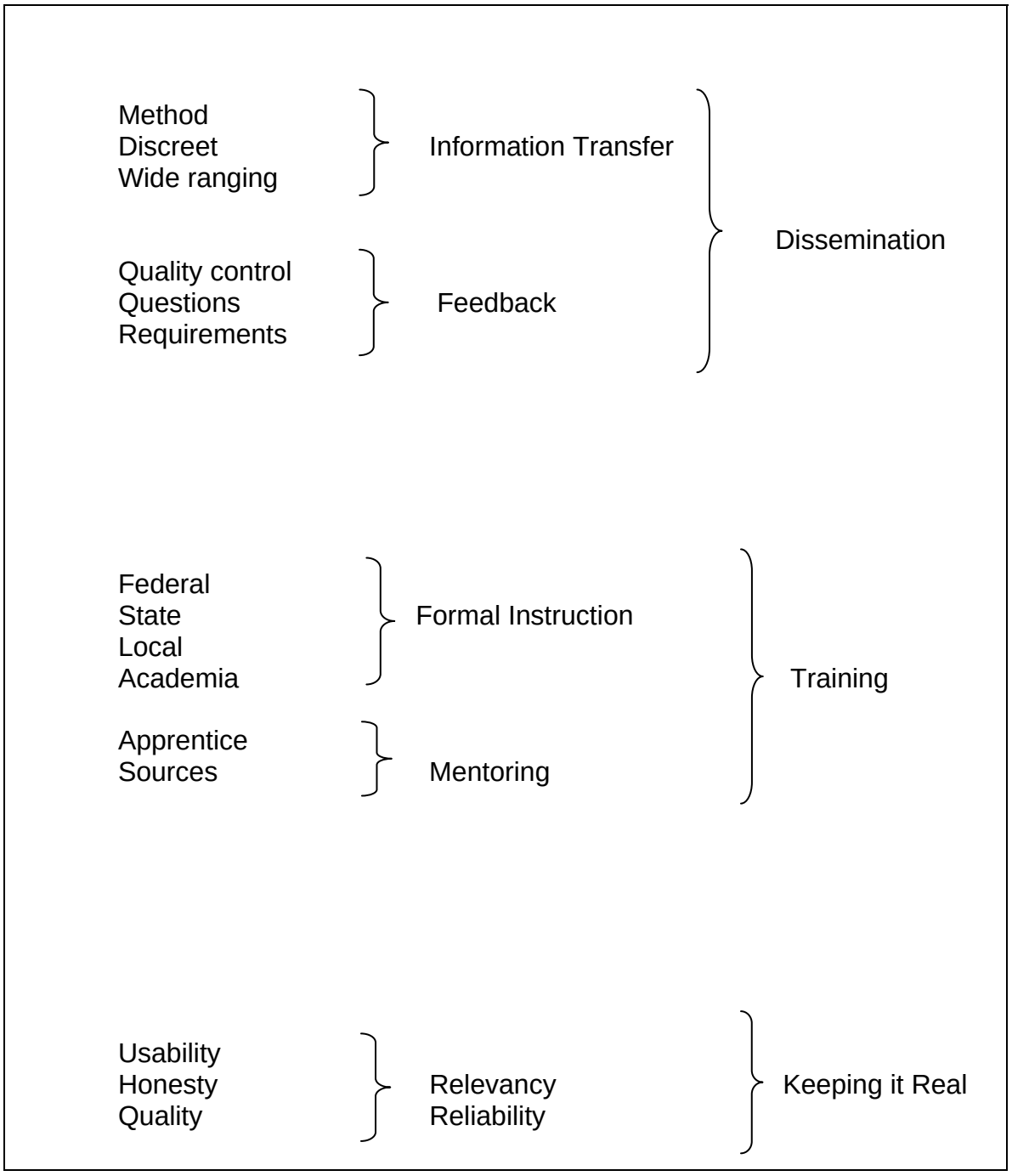


Figure 1. Emergent Analytical Codes and Categories

2. Writing

The data from the interviews was interpreted by the researcher in light of the needs of the fire service without getting too far from the ideas and

experiences of the subject matter experts. Most importantly, the researcher sought to avoid a theoretical approach and instead attempted to provide useable information arising out of the first hand experience of the involved intelligence professionals. It is the researcher's fondest hope that this thesis is actionable by the fire service in understanding and using intelligence. In writing this thesis, the advice of Rubin and Rubin has been followed, which is to use extensive quotations from the interviews in order to make the interviewees real.[48]

[48] Herbert J. Rubin and Irene S. Rubin, *Qualitative Interviewing The Art of Hearing Data*, 2nd ed. (Sage Publications, Thousand Oaks, CA, 2005), 252.

THIS PAGE INTENTIONALLY LEFT BLANK

III. DATA ANALYSIS

A. INTELLIGENCE

1. Purpose

What is the purpose of forming a fire department intelligence unit? The answer is simple; to protect the members of a department and the community they serve. Francis Bacon, the 17th century English philosopher, once said that knowledge is power. The fire service has always known this to be true. Firefighters learn hydraulics, building construction, emergency medicine, line placement, hazmat, and so many other topics because this knowledge gives them the power to do their jobs properly. "Good information allows for good decision-making. Bad information or a lack of information always results in poor decision-making."[49]. An intelligence unit has the same function, except in the field of terrorism. When asked what he saw as the purpose of a fire department intelligence unit, Fred Burton replied, "Well, you're going to make your department better educated, better informed, better trained, more cognoscente of the life safety threats, the risks you run. With an intelligence shop, you are going to make your fire fighters smarter and your command staff better informed. You, at the end of the day, may even save lives by having analytical assessments done on your first due response areas."[50] Later in the interview, he explained its all about, "life safety, meaning we are going to create an intelligence analytical capacity within (the department) in order to save lives, period. We're going to serve the civilian population better because we're going to do intelligence-led fire fighting versus reactive fire fighting."[51] This is the ultimate purpose of any fire department intelligence unit.

[49] "Fire Department Intelligence Officer," *FDSOA Safety-Gram* 15 (February 2007): 1.

[50] Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

[51] Ibid.

Of course, having a fire department intelligence unit does not guarantee safety and there are costs to having such a program. So, why do it? Speaking of terrorism, George Friedman stated, "Most of it won't come here (the United States). And some of it may come here (and) we will not be prepared for it. What you're trying to do is cut the odds down."[52] Intelligence is not a panacea. It is not foolproof; however, intelligence has a real value, perhaps life saving value, to the local fire department and every department from the largest municipal agency to the smallest volunteer organization should have an intelligence unit or at least an intelligence officer who looks at terrorism and says how might this affect my department; how might this affect my locale? "The point is that good intelligence is cheap in a sense that it doesn't have a tremendous amount of bells and whistles."[53]

Fire departments should be thinking about and planning their response to a potential terrorist attack. They owe it to themselves and to their communities. Unfortunately, terrorism is going to be around for a long time. The intelligence unit or officer should also be used in strategic and tactical planning as an information source. For instance, hotels have become a major terrorist target around the world. They are a soft target that is easy target. There have been major terrorist attacks against hotels in Amman, Jordan, Islamabad, Pakistan, and Mumbai, India. The attacks have caused craters in the street interfering with the positioning of apparatus, mass causalities, gas leaks, fires, and structural collapse. What are your department's plans if an attack should happen in your city, town, or village? Developing plans to respond to such a situation at a hotel or other soft targets in your response area is one of the times brainstorming and the involvement of several chief officers may be required; however, the intelligence office should be able to find a lot of information on these attacks and the damage that they cause. This will help a department keep its planning realistic. How many hotels or other soft targets exist in your geographic area?

[52] George Friedman, interview by author, field notes, Austin, Texas, November 19, 2008.

[53] Ibid.

Do you have floor plans, and site maps? Does you department know what auxiliary fire protection equipment is present? What is the back-up plan if these systems are rendered inoperable? All these items can be collected by the intelligence office for planning purposes.

2. Open Source Intelligence

Though secret and top secret intelligence may, at first, seem to be the most attractive, it is not the most useful form of intelligence for the fire service. Since most fire department personnel do not have security clearances and the process of getting clearances is long and cumbersome, the most useful type of intelligence information is open source intelligence (OSINT), especially since most fire departments will want to disseminate received intelligence information to all of its members. "Due to its unclassified nature, OSINT can be shared extensively without compromising national security."[54] Information that cannot be shared with the units in the field may have limited value.

The interviewees were almost unanimous in their belief that secret and top secret intelligence was not required for the fire service. However, even unclassified open source intelligence may create difficulties for the average fire department because most are not currently equipped to handle it. Assuming that the local fire department is receiving intelligence, the flow of information coming from the Federal government and local fusion centers may be massive and requires additional processing by fire departments to exploit this intelligence properly. This is because, currently, much of the information flow is not specific or useful to the fire service. Much of it tends to be for use by the law enforcement community. Hence, a local fire department needs to put an analytical mechanism in place to separate out what is useful from this information flow, the signal-to-noise problem. Therefore, the local fire department needs

[54] Eliot Jardines, *Using Open Source Information Effectively: Hearing Before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security of the House of Representatives June 21, 2005* (Washington, D.C.: U.S. Government Printing Office, 2007), 13.

specifically trained personnel and systems to accomplish this processing and analysis. Most fire departments do not have the systems or the personnel in place properly to utilize OSINT, nor do they have the experience to build such systems. The interviewees gave of their time and the benefit of their expertise in order to help the fire service build those systems. The following chapters are meant to assist a fire department that sees the value of good intelligence and situational awareness to begin to build the required structures and expertise.

3. The Intelligence Cycle

Even though the intelligence cycle is somewhat of an artificial construct, it has been used in this thesis because it provides a useful framework in which to discuss intelligence. All of the steps of the intelligence cycle may be going on at the same time; some steps may not be as clear-cut as they are made out to be in the literature. It is important to remember that the intelligence cycle is iterative. The products a unit develops may lead to other questions and then to other products. Nevertheless, an intelligence unit needs to give some thought about each of these steps in order to produce a worthwhile and useable product. In addition, it will allow personnel in a fire department intelligence unit to communicate using a common language with intelligence analysts in other fields. This intelligence cycle architecture was certainly helpful in the interviews with the subject matter experts. Figure 2 presents a descriptive précis of these steps, including some illustrative quotes.

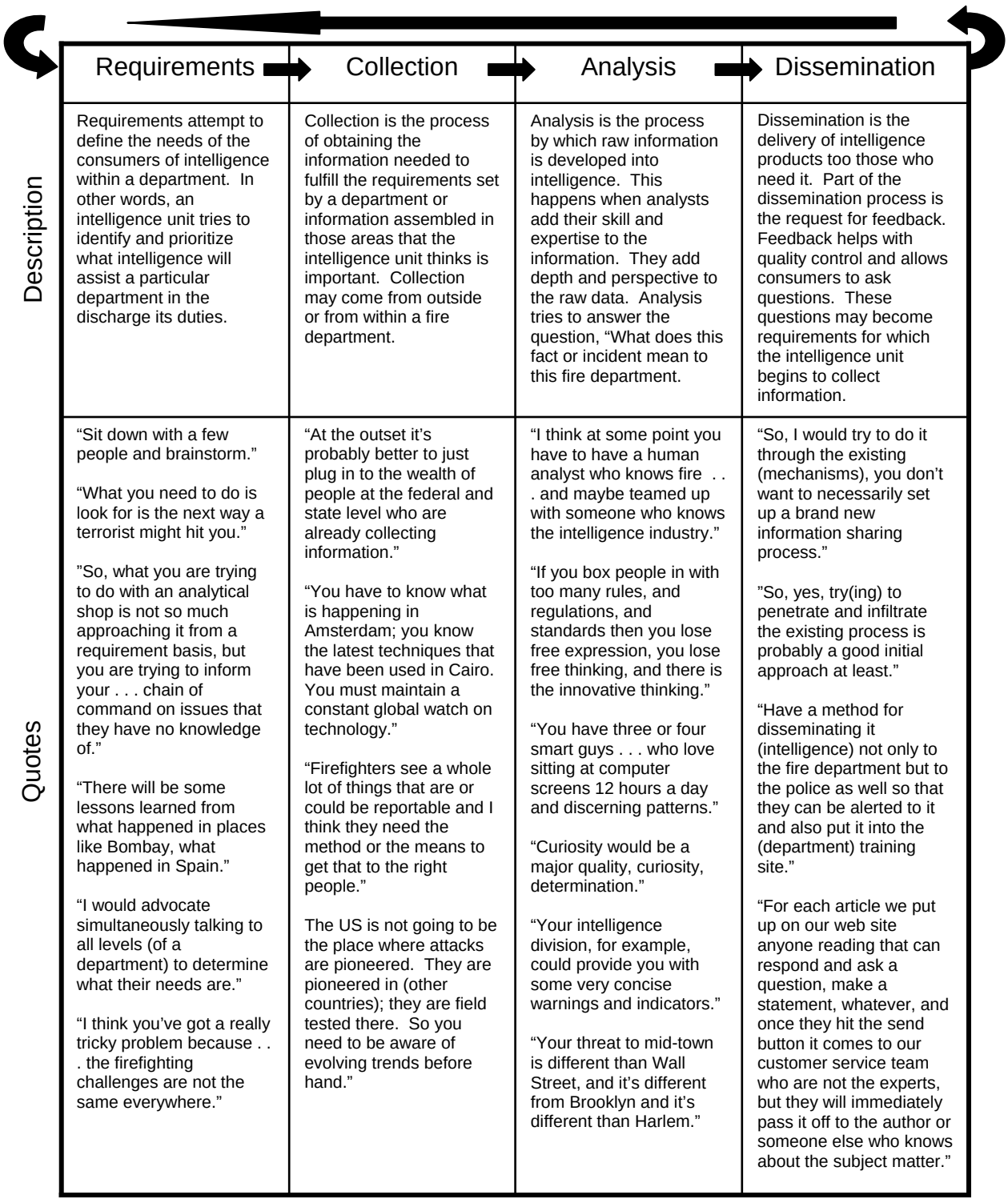


Figure 2. Stages of the Intelligence Cycle: Description and Representative Quotes

B. REQUIREMENTS

The most important step in the intelligence cycle is to define what a particular organization or policy maker needs to know. No other step in the cycle can be performed until these needs are established and all the work that might be put into the subsequent steps of the intelligence process is wasted if policy makers and the members of a department get junk information because no well thought-out intelligence needs have been established. Setting requirements is not only the most important issue a department needs to determine, but also generally, the most difficult one. It is an even more difficult question for the fire service since intelligence requirements need to be defined on a local level and the local fire department often the lacks the experience with intelligence to tackle this task. As John McCreary said, "I think you've got a really very tricky problem because . . . the firefighting challenges are not the same everywhere."[55] Yet, the question of defining intelligence requirements is critical and needs to be carefully considered by the local department.

The intelligence professionals interviewed had several ideas on how a local fire department should begin to define its intelligence requirements. Not all of the interviewees agreed with each other on how they would perform this function; however, almost all stressed its importance. On the other hand, the ideas they tendered were not necessarily mutually exclusive; a local department may wish to try a blended approach, using several ideas below to establish its requirements. Departments should not be afraid to change its requirements creation process if the existing system is not working as well as it should. Additionally, a department can and must update its requirements as the local environment evolves.

1. Brainstorming

Brainstorming is an important part of this process. One of the interviewees said that if he were hired to start an intelligence office for a fire

[55] John McCreary, interview by author, transcript, Washington, D.C., November 25, 2008.

department he would "sit down with a few people and brainstorm."[56] As an outsider coming into the fire service, he would take "some time to observe, and listen, and talk to the people who do the work, not only the firefighters on the line but the investigators;" "this is pretty much step one."[57] Mr. Johnson points out that each level of command has their own need and he advocates, "Simultaneously talking to all of these levels to determine what their needs are."[58] Only then, can one connect the thoughts and determine where information can be effective in helping a department fulfill its role in protecting a community against terrorism.[59] This is good advice for anyone tasked with deciding a department's intelligence requirements, even those experienced in the fire service.

2. Freedom

Another school of thought says, "in essence, they (the local fire department) don't know what they don't know, meaning how do you create a requirement based upon an intelligence gap?"[60] In other words, it is very difficult for a department to set its requirements, since "it doesn't know what it doesn't know." Fred Burton stated that a department might know where every hydrant is on a street, and send someone out to test them and make notifications if one is down, "but you may not be aware of the real threat that lies on that street."[61] How does one solve this problem? The answer is pick good analysts and allow them the freedom to discover the real threats. These analysts pick their issues without undo interference from the higher echelons of a department. "What you're doing with an analytical shop is not so much approaching it from a requirements based (system), but trying to inform your managers and your

[56] Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

[57] Ibid.

[58] Ibid.

[59] Ibid.

[60] Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

[61] Ibid.

bosses and your chain of command on issues that they have no knowledge of whatsoever."[62] In other words, rather than trying to set up formal requirements, a department is really depending on its analysts to come up with answers to questions that nobody has thought of as yet.

These two systems are not necessarily in opposition to each other. A department could establish some formal requirements for its analytical unit to handle. These would be established through brainstorming and discussion with each level of a department in order to see what intelligence is necessary to respond to terrorism as safely as is possible. Yet at the same time, the analysts could be given the freedom to answer questions that nobody has asked, but that the analytical team thinks is important. This is because a department may need "to know those things that somebody hasn't sat around and thought of" yet.[63]

The alternative to locally defining requirements is to allow other agencies to give whatever intelligence they deem relevant and hope that the fire department receives the right information. This school of thought says that since fire departments may not have their own analysts, they "should be receiving properly analyzed and corroborated information, unless that information relates to an imminent incident or threat."[64] On the other hand, locally specific, well thought-out intelligence requirements would also help the Department of Homeland Security (DHS) and other federal entities fulfill their missions within the National Information Sharing Strategy, while not overwhelming the local fire service with large quantities of information of limited relevancy.

3. Guidelines

Below are some additional ideas on helping a local department establish what it needs to know. First, any intelligence requirement produced by the fire service must support its core mission. The core mission of any fire department is

[62] Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

[63] Ibid.

[64] Fire Service Intelligence Enterprise (FSIE), *Progress Report 1* (December 28, 2008), I-2.

protecting life and secondarily protecting property in their community; these are the raison d'être of the fire service. For instance, the "the core mission of the FDNY is life safety."[65] If the proposed requirements do not directly support a department's mandate to protect life and property, they are faulty. For instance, knowing the strategic balance between the United States and a resurgent Russia may be important, even critical, to the national security of the United States, but such intelligence is probably not necessary for the fire service to protect the citizens of its local community. On the other hand, a department may want to know about the latest terrorist attacks in India.

Further, intelligence is not primarily an intellectual exercise, meaning that the information requested should not be "interesting," but "useful." Therefore, the second standard for a fire service intelligence requirement is that it should be useable. Lowenthal makes the point that policy makers "seek intelligence that is actionable intelligence, that is, intelligence with which they can do something."[66] This desire for actionable intelligence is just as true for the fire service. Hence, intelligence that has no practical application is of little value to any department.

The third requirement for intelligence is timeliness. Intelligence must not be received after it is no longer useful. The timing of intelligence may be broken into two broad categories. Long-term intelligence should be more in depth and looks at what may happen in one month to several years. Long-term intelligence is also known as strategic and operational level intelligence. This type of intelligence is useful to the fire service because it allows for longer term planning for equipment purchases; it allows time to create and implement necessary training, and permits drills to be carried out. Additionally, departments can craft better standard operating procedures if it has an idea of how terrorist groups may act. Short-term intelligence involves warnings of an imminent attack. Short-term or tactical intelligence may cover the period of one day or less to several weeks.

[65] Fire Service Intelligence Enterprise (FSIE), *Progress Report 1* (December 28, 2008), 13.

[66] Mark M. Lowenthal, *Intelligence from Secrets to Policy*, 3rd ed. (Washington, D.C.: CQ Press, 2006), 234.

In this period, there may be little occasion for a department to prepare thoroughly for the attack. However, staffing levels may be increased and curtailment of nonessential fire service activities initiated.[67]

Given these provisos, what kinds of intelligence does the local fire service need? The answer is simple; a local fire department needs good situational awareness. The department needs to know what is going on in the world of terrorism. What is happening strategically and tactically with terrorist groups? This information may come from other countries or it may cover what is happening in the United States. Most importantly, what is the possibility of an attack on their local community? How will it most likely happen? Are there changes in terrorist tactics that the fire service should know about? Are there signs or warnings of imminent attack? What types of improvised explosive devices (IEDs) are being used around the world? How are these IEDs being used? For instance, George Friedman stated, "What you need to look for is the next way a terrorist might hit you. Okay so cell phone detonated bombs, well they are old hat now, but coming along is some other really nasty thing."[68] This is what the local fire service needs someone to be looking for. Is there an increasing amount of secondary attacks? Have there been attacks specifically against fire departments? In other words, what is going to hurt your department and the people you serve?

Attacks from around the world need to be examined in light of a local fire department's community. A department needs to look at the implications of foreign and domestic attacks with an eye to how that particular department operates. Attacks that take place in the United States will probably have been tested in other parts of the world. "As part of this effort," a department should realize "there will be some lessons learned from what is happening in places like Bombay, and what happened in Spain."[69]

[67] Fire Service Intelligence Enterprise (FSIE), *Progress Report 1* (December 28, 2008), I-2.

[68] George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

[69] John McCreary, interview by author, transcript, Washington, D.C., November 25, 2008.

Weapons of mass destruction are another area of concern. Though they may have a low probability of use, they have the potential for high causalities as well as potential for extensive property and economic damage to a locale. Any long or short-term intelligence federal or state agencies can supply may help departments prevent, prepare for, or mitigate such an attack.

Cyber attacks, though they may not seem like a fire service issue, may adversely affect the fire department of a community. Many fire departments dispatch their units by computer assisted dispatch systems. Any damage to those systems would force a return to manual dispatch systems, which are more labor intensive. Departments may need to assign additional dispatchers to their communications office to prevent the collapse of dispatch operations. Additionally, many forms of cyber attack may hugely increase utilization of departmental assets. For instance, more and more elevators are being tied into centralized computer systems for operation, maintenance, and repair. A cyber attack on these computers may result in literally thousands of people being trapped in elevators and requesting fire department assistance. Cyber attacks on utilities may cause similarly widespread problems. Any intelligence that could either help departments to protect its systems or give it forewarning of targeted attacks may help it prepare to respond.

Another intelligence requirement is threats to infrastructure. This intelligence should not be limited to a particular city or town because most locations are dependent on such things as water and electricity from outside its own borders. This information may allow a department to do contingency planning on how it will operate if it lost the use of a specific infrastructure. One of the most important things a department needs to know about is threats to their water supply.[70] Firefighting activities generally come to an end without water.

In summary, although some interviewees distrusted formal requirements, an example list of fire service intelligence requirements could be the following.

[70] John McCreary, interview by author, transcript, Washington, D.C., November 25, 2008.

- Situational awareness and terrorist threats
- Improvised explosive devices
- Weapons of mass destruction
- Cyber attacks
- Threats to infrastructure

C. COLLECTION

Does a fire department need to go out and begin its own raw collection? In other words, does the fire service need to hire and run agents on the street? The answer, of course, is no; that is not what this thesis is suggesting. It would be both cost prohibitive and inappropriate to attempt this kind of collection. In addition to the potential legal difficulties, it would be beyond the scope of the fire service's mission to attempt to do so. So, then, how does a fire department intelligence unit find information in order to fulfill its mission? It might be less of a problem than most think. Indeed, the real problem is not so much that there is not enough information out there; the problem is that there is too much data. The difficulty is that "there is too much information out there to make sense of it logically because today we are inundated with information."[71]

1. External Sources

The information to collect is that which supports the fire service's mission to protect life and property in its local community. Therefore, a good place to start is to have an intelligence unit or intelligence officer liaison with the local police department. The local police usually has a finger on the pulse of the local community. There may be state and local police in a particular area and a fire department should make contact with all of them. In addition to being able to supply information that may be of use to a department, the personnel involved become familiar to each other. Then if an emergency occurs, the agencies are not strangers but have, ideally, already built a level of trust with each other. Pat

[71] Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

Miller stated, “Because they (the police department) are tied into so many different systems that the fire department isn’t, that’s where you need to start.”[72]

All appendices are restricted.

The next set of people to make contact with is the U.S. Department of Homeland Security’s Protective Security Advisors (see Appendix A). “In 2004, the Risk Management Division (RMD) Field Operations Branch (FOB), established the Protective Security Advisor (PSA) Program, deploying a cadre of 68 critical infrastructure security specialists, with an average of 20 years of law enforcement, military, and anti-terrorism experience, permanently assigned to 60 metropolitan areas designated as PSA districts across the United States.”[73] One of the areas where a fire department’s intelligence unit can be helpful to its department is in the area of critical infrastructure in a local community. Where is it? What are their dangers? Would this facility create any special difficulties in firefighting or hazmat response if it were involved in a terrorist attack or other disaster? The intelligence unit should be asking these questions. Pre-operational planning should result from this research. The local PSA is a valuable source of information and can make introductions where necessary to local critical infrastructure operators. This is significant because local infrastructure operators are experts with unique insights into their facilities; they are an important resource. Additionally, PSAs act as a line of communication between the local community and the Department of Homeland Security in the area of potential threats, and they can help with exercise design in their geographical area. The intelligence unit can use this assistance if it is called upon to set up drills for its department.

[72] Pat Miller, interview by author, field notes, South Bend, Indiana, November 22, 2008.

[73] “Protective Security Advisor Program Overview,” http://www.cops.usdoj.gov/files/ric/CDROMs/PlanningSecurity/modules/11/Module11_ProtectiveSecurityAdvisor.pdf (accessed January 16, 2009).

Additionally many states have homeland security departments. A fire department intelligence unit should make contact with them and see what services these agencies might have available. "The homeland security (agencies) at the state level . . . have a broader view of things and they are not just law enforcement, they're also first responder."[74]

Next, the intelligence officer of unit should make contact with the local or regional fusion center (see Appendix B). They may well be a great source of information. However, the unit should not become overly dependent on the fusion center alone. There are several problems with the fusion centers. One is that their future is uncertain. In addition, the quality and scope of their work is uneven. There is a saying that goes, "You've seen one fusion center, you've seen one fusion center." In other words, each fusion center is unique both in terms of what it fuses and in terms of how well it does it. The other problem is that fusion centers tend, with few exceptions, to be law enforcement focused. "And everybody else including the fire department is kind of a second team. If they participate they do, but we (the fusion centers) don't care if they don't."[75] Some of the interviewees also questioned the usefulness of many of the products the fusion centers generate to emergency personnel on the street. Others thought they might be useful. "Fusion centers can be useful provided everyone shares information. Across the country, you will find various opinions as to the usefulness due to turf issues. I see duplicate efforts in a lot of places."[76] Due to these limitations, a fusion center should not be a department's only source of information.

This is not to say that one should not contact and use the local fusion center. An analysis unit absolutely should. Indeed, one suggested alternative to a fire department having its own intelligence unit is to place firefighters in the regional fusion center as analysts. "A couple of people who have a firefighting

[74] Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

[75] Pat Miller, interview by author, field notes, South Bend, Indiana, November 22, 2008.

[76] Fred Burton, e-mail message to author, January 19, 2009.

background" could "establish a firefighting intelligence desk or something at the fusion center and their job would be to look through all the flows of information coming in a pull out the relevant things to the firefighters, to the first responders, and the allied disciplines."[77] Some fusion centers are doing this. However, that still leaves the need for the local fire department intelligence unit to look at the materials posted by their fusion center and see how it applies to their department, with its particular infrastructure, and its particular policies and procedures.

There is a wealth of information and processed intelligence available on the internet (Appendix C). Most of these web sites require that a department apply for access to them. The information they contain is voluminous and covers just about every aspect of terrorism. For instance, the Overseas Advisory Council (OSAC) does good analysis of what is happening around the world and creates excellent PowerPoint presentations on major terrorist attacks around the world. "You have to know what is happening in Amsterdam; you have to know the latest techniques being used in Cairo. You must maintain a constant global watch on technology."[78] A department needs to "watch the technologies that are evolving in other parts of the world. The U.S. is not going to be the place where attacks are pioneered. They are pioneered in (other countries) – they are field tested there. So you need to be aware of evolving trends before hand."[79] This knowledge should support one's training for a response to a terrorist incident. Others like the Universal Adversary Portal contains information on terrorist groups and information that is helpful in exercise planning. This includes terrorist groups that operate within the United States. This is because a fire department must also look within the country at terrorist trends as well. "9/11 showed us you

[77] Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

[78] George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

[79] Ibid.

can't just focus on overseas; a focus only on overseas doesn't necessarily guarantee security."[80] Still others sites contain information on such topics as critical infrastructure and weapons of mass destruction.

The Open Source Center (https://www.opensource.gov/) site is especially helpful because it has a subscription service that will e-mail the intelligence unit materials that they request. This is an example of a pull site; the user pulls what they think useful to their organization.[81] A fire department analyst should think about the subscriptions they might find useful. Certainly, words such as "fire department," "arson," "fire bombings," "improvised incendiary devices," and "terrorism" should be included in the subscription. Additionally, an analysis unit should request that the Open Source Center send them anything that mentions the name of their state or locality. Two entities are especially useful to the fire service because they are more fire related than most sites. One is the Emergency Management and Response Information Sharing and Analysis Center site (EMR-ISAC), which is run by the U.S. Fire Administration. This site will send e-mails and infograms with emergency sector specific intelligence and information. Chief Officers may receive Sensitive CIP Notices, which are "For Official Use Only."[82] The other is Watch Line, a product of the Fire Department of the City of New York's Center for Terrorism and Disaster Preparedness. The Center produces it weekly and is a good vehicle for fire departments that are trying to improve their situational awareness. Almost all of the information in Watch Line is useful to the fire service.

The members of the intelligence and analysis unit should always be making connections. Every time members of the unit go for training, every time its members go to a conference, talk to other people at the training event, the speakers, and the instructors; make contacts. Get a business card if possible;

[80] John McCreary, interview by author, field notes, Washington, D.C., November 25, 2008.

[81] Mark Johnson, interview by author, field notes, Washington, D.C., November 4, 2008.

[82] Charles Werner, "Progress Report: Information, Intelligence for the Fire Service," Firehouse 29 (December 2004), 40.

file the card. Jot a few notes about the person or agency on the back of the card. Do not just do this for other fire departments. A department might want to do this with federal and police agencies, infrastructure operators, the radiation hygienist at the local hospital. The unit must use its imagination. Get anyone and everyone's card. You never know when that contact might help your department. Thus, if a question arises or something happens in another locale, the intelligence unit can contact that person and get the straight story. It is suggested that this be done even if it is necessary to make contact with another fire department in another state. On the flip side, have a business card available and give it out. Help where possible. Networking can be invaluable to an intelligence unit.

Lastly, some of the interviewees suggested that the intelligence unit could collect raw material right off of the internet. For instance, Mark Johnson gave an example, "I'll bet if you go on YouTube today and type in, how to set a fire using whatever or how to build a bomb, you are going to find videos on there that tell you that and some could be . . . in the (department's) region or city."[83] A contractor can set up a web crawler to look for these kinds of materials in a particular area or nationwide. The intelligence unit would need to review these materials to see if they have any value. However, this level of sophistication is probably beyond the scope and abilities of most fire department analytical units.

2. Internal Resources

There is another source of information for the intelligence unit that should not be ignored. That is the members of one's own department. The 316,950 professional and 823,950 volunteer firefighters in the United States enter thousands of buildings on a daily basis.[84] Firefighting personnel enter residences, factories, warehouses and apartment buildings for fires, medical

[83] Mark Johnson, interview by author, transcripts, Washington, D.C., November 4, 2008.

[84] United States Fire Administration, Federal Emergency Management Agency, "Firefighters," http://www.usfa.dhs.gov/statistics/firefighters/index.shtm (accessed August 31, 2008).

emergencies, utility emergencies (gas, electric, water), and to accomplish building inspections. "Unlike police, firefighters and emergency medical personnel are not required to obtain a warrant to enter a building."[85] Each of these inspections and responses is a potential opportunity to gather intelligence on terrorists who may be operating within the local community. George Friedman of Stratfor stated, "I regard firemen not policemen as the first line of intelligence across the board."[86] For instance in April 2005, in the course of a routine building inspection in Brooklyn New York, members of the F.D.N.Y. found more than 200 airbags in the basement of a food market that also had newspaper clippings about Osama bin Laden and beheadings in Iraq covering the walls.[87] Now, purportedly this incident was not related to terrorism; however, in addition to the obvious clippings, firefighters realized that airbags contain an explosive charge, sodium azide, which could be used by terrorists.

The important point here is that information received by the fire service and disseminated by the local department's intelligence unit increases its situational awareness, thereby, increasing its ability to recognize terrorist activity. In addition, there may also be times when federal or local police agencies have specific things they desire a local fire department to be looking out for in the course of its normal duties. Firefighters and EMS personnel must have a clear reporting mechanism for any information collected. The department's intelligence unit or intelligence officer is the natural choice for this liaison function.

The intelligence unit also needs to work with the department's training division in order to instruct firefighters on what they should look for or perhaps the unit needs to do the training directly. "Firefighter's can be plugged into the training regime and you (the intelligence unit) can do annual refreshers, you can do quarterly updates, what's new and overseas bombing overseas and other

[85] Richard Blatus, *Altering the Mission Statement: The Training of Firefighters as Intelligence Gatherers* (Master's Thesis, Naval Postgraduate School, 2008), 5.

[86] George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

[87] Rich Calder and Murray Weiss, "Stash 'Bagged' at Market," *New York Post*, April 27, 2005.

events. You (the intelligence unit) may see trends and you have got to communicate with the people . . ."[88] A firefighter cannot collect information if he or she does not know what to seek.

Another aspect of a fire department's collection is human intelligence. Again, running agents and informants on the street is not what is being recommended here. What is recommended is that firefighters be trained to report what they hear on the street if it involves potential terrorist activity. George Friedman commented that if he were in charge of a fire department intelligence unit, "I would create . . . a human intelligence network. And for me a fire department is superbly located. It's in the community, it's in every community. It's a non-threatening entity and your people (firefighters) have constant daily interactions with the community including stakeholders in the community, which would not just be gang members, (but) people who own stores and so on."[89] The difference here is one of actively running an intelligence operation versus a firefighter knowing enough to report what they hear passively.

People might well be willing to talk to firefighters who are not willing to talk to the police. The community should know that they can talk to firefighters if they suspect terrorism. "The cops are feared. I'm afraid of them. Firemen are benign. They're the people who come to your house when you've had a heart attack. They're the people who will save your kids when they have done something really stupid climbing up somewhere."[90] This is not to say that this trust should be abused; however, firefighters should be trained to listen. "Your guys are in neighborhoods . . . where somebody might tell you, 'You know don't tell anybody but my cousin is kind of insane and I don't know what he has in his bedroom, but it smells bad.'"[91] Firefighters should be trained and motivated to report something like this.

[88] Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

[89] George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

[90] Ibid.

[91] Ibid.

A department's emergence medical response personnel should be trained as well. They might see injuries that are unusual. If terrorists are using chemicals to produce explosives or chemical warfare agents and something goes wrong, medical response personnel should be trained to notice the atypical injury. Does the story behind the injury match the injury; is the injury really weird? One interviewee asked, "Where does the (report of) interesting wounds, the burns that don't make sense, acid burns that don't make sense, shrapnel wounds in the leg" get directed to? "Because that's how you are going to find a terrorist cell. Some - - is going to do something boneheaded with one of his systems, cause a fire, cause a wound to himself and so on."[92]

Multiple interviewees emphasized the importance of having a clear reporting mechanism. It might be as simple as putting a poster on the wall of the firehouse with a telephone number and most importantly someone on the other end who can answer questions or take the information.[93] The success of a department's firefighters serving as extra eyes and ears will only be successful if the local department "establishes a procedure and a format where firefighters would be able to know what to look for and how to report it."[94] Some cities have such a system in place. Again, the intelligence unit is the natural point of contact for these suspicious activity reports, especially since it might be able to fit the report within the larger context of what is occurring with terrorism in the region and the world. The intelligence unit, by the contacts they have previously made, should know who to pass this information onto in the local police and Federal Bureau of Investigation.

Several of the interviewees stressed the need for the system to be simple and have a reward system in place. This is not to suggest cash rewards or the like; however, "they (department personnel) need to know that what they are

[92] George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

[93] Ibid.

[94] Pat Miller, interview by author, transcript, South Bend, Indiana, November 22, 2008.

doing matters."[95] Every report gets a response. Even if there is already an ongoing investigation and the fire department intelligence unit cannot reveal the specifics of a case, the reporting personnel still get an individual telephone call from the unit thanking them for the report. This tells department personnel that someone is listening, someone is responding to their report. They are not wasting their time. Failure to respond will cause the failure of this effort. If the process is not simple or firefighters never hear anything back on the reports they file, "people aren't going to take the time or they'll do it once and say screw this."[96]

However, this is not to say that firefighters should become intelligence agents for the federal government or police officers. This would create both constitutional and public relations problems. In November 2007, the American Civil Liberties Union attacked the FDNY for its reported "training" in intelligence gathering. The ACLU spokesperson asked do we want people "to fear the fire department as well as the police."[97] While the question is unfair, it does contain a word of caution. The fire service must remain scrupulously within the limits of the law while still performing this vital function. Of course, a "fire department must guard against drifting into law-enforcement activities – namely, investigating crimes and apprehending criminals."[98] Indeed, even with meticulous attention to the legal issues, there may be a political backlash to a closer relationship with police and federal intelligence agencies. Nevertheless, terrorism prevention is clearly a part of the fire service's life safety mandate.

There is another downside to firefighters acting as intelligence collectors. There would need to be a commitment to training fire department personnel in the recognition of the signs of potential terrorist activity. This would require a

[95] George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

[96] Pat Miller, interview by author, transcript, South Bend, Indiana, November 22, 2008.

[97] MSNBC, November 23, 2007, http://www.msnbc.msn.com/id/21940968/page/2/ (accessed August 31, 2008).

[98] Kyle Dabruzzi and Daveed Gartenstein-Ross, "Firefighters' Developing Role in Counter Terrorism," *Policing Terrorism Report* 3 (July 2008): 2.

portion of a department's limited training time that one could argue would be better spent preparing for fires and emergencies. Nevertheless, whatever the public relations problem, and whatever the necessary commitment of resources, they must not deter the fire service from exchanging lawful information with other agencies. Such a two-way passing of information and intelligence helps the fire service to fulfill its sworn duty to protect its citizens, their fellow first responders, and themselves from a terrorist incident. Secondarily, a local fire department must protect the property and economic resources of its community. The fire service's obligation to "protect life and property" supersedes any potential downside to firefighters keeping their eyes open in the course of their normal duties.

In summary, a fire department intelligence unit collects information from multiple sources. Its staff forms relationships with personnel in other agencies in support of its mission. John McCreary said of this unit, "What you guys have to do is set up a liaison core."[99] The intelligence unit should not just be sitting in an office. In addition, it uses online resources supplied by the local fusion center, the Department of Homeland Security, and federal law enforcement and intelligence agencies to find applicable material. They obtain information from the members of their own department. Collection is a function that requires imagination and adaptability. Imagination is the only limit to where and what types of information can be collected.

D. ANALYSIS

Intelligence is more than just gathered facts. An analyst is more than just a person who collects information and passes it along to someone else. The analyst or analytical team must know what is important to the people or the organization they serve. With this in mind, they collect information and add value. The value they add is their own expertise. They add depth of meaning and insight. More than just facts, they try to give an understanding of what these

[99] John McCreary, interview by author, transcript, Washington, D.C., November 25, 2008.

facts could mean to their consumers. How does this individual or team help a fire department manager? Fred Burton posited, "I don't have time to read . . . 25 different websites and six different E-mail providers a day. So, your analytical shop, your intelligence division, for example, could provide you with some very concise warning and indicators, information as to what you should be thinking about, not only from a tactical perspective, but a strategic perspective."[100]

1. Uncertainty

This does not imply there is only one possible explanation of what some piece of information could mean; sometimes there may be several competing explanations for a set of facts. An efficient group of analysts may explain the strongest possibilities and discuss the implications of each. Additionally, in most cases, there will be incomplete data on a particular topic. This does not mean that an analyst should not evaluate the existing information, but it does mean that they should convey the level uncertainty. "One way to help convey uncertainty is to identify in the analysis the issues about which there is uncertainty or the intelligence that is essentially missing but which would, in the analyst's view, either resolve the unknowns or cause him to reexamine currently held views."[101] How does a local fire department do all of this? Where does it obtain the requisite analytical expertise?

2. Team Approach

Almost all interviewees agreed that a team approach to analysis would be the ideal way of proceeding. Mark Johnson said, "I think at some point you have to have a human analyst who knows fire, knows the firefighting trade, industry, and maybe teamed up with someone who knows the intelligence industry."[102]

[100] Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

[101] Mark M. Lowenthal, *Intelligence from Secrets to Policy*, 3rd ed. (Washington, D.C., CQ Press, 2006), 129.

[102] Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

Pat Miller reported, "You will have to bring in someone with an intelligence background, I think, in order to do it right."[103] Why should this be so?

> Setting up interdisciplinary teams is a method that we often use to tackle tough questions. In fact, to carry it out into the ultimate . . . the National Counterterrorism Center is an interdisciplinary team. You've got FBI analysts up there, you've got CIA case officers who run spies overseas; you've got CIA analysts who are experts in cultural things, You've got DIA people who specialize in military intelligence, and you've got a whole host of others. So, I think that (the) principle is applicable at all levels down to a fire department. You need both, you need it all.[104]

No one person can know it all; that is why the team approach is a good paradigm for fire service intelligence. John McCreary, an experienced intelligence professional said, "I'd have to work, sit with a knowledgeable firefighter," I'd have "to learn from him as well as see if I can apply what you need to know."[105] A team approach is ideal; however, it is not the only approach, especially if a local department does not have the resources to include an outside intelligence analyst.

How, then, does a department choose fire personnel to place into an intelligence team? What qualities does one look for in a potential analyst chosen from within a fire department? Choosing the right person is especially important for a department that may not have anyone with an intelligence background available either from within or from outside the department. The most basic answer is to choose for quality of mind. Irrespective of all other qualifications, department leadership has to look at the intellectual qualities of the individual. Obviously, the individual would also have to have an interest in the intelligence field, and certainly, expertise in certain fields such as improvised explosive devices would increase the value of an individual to a department.

[103] Pat Miller, interview by author, transcript, South Bend, Indiana, November 22, 2008.

[104] Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

[105] John McCreary, interview by author, transcript, Washington, D.C., November 25, 2008.

A department could make several errors in choosing an analyst, as many firefighters may not be suitable for this role. Firefighters, as a general rule, tend to be process oriented and this is not the ideal way to do intelligence. One mistake would be to take a firefighter on light duty and "make him the analyst this month. That's a very good bureaucratic move. (However), it doesn't help generate your intelligence products."[106] Another error would be to choose analysts by rank or seniority in a department. "You could be successful at pulling it off if you had the right mindset and leadership meaning if you selected not based on seniority, not based on Vinnie's cousin . . . throw out your seniority, throw out your rank. I'm not saying (don't) have a boss," but your lead analyst "may be 20 years younger than the people that ultimately would work in the unit."[107] In other words, a fire department needs to make a careful choice of individuals, ones with the right qualities, irrespective of extrinsic factors.

There are many positive qualities a department should look for in personnel assigned to this enterprise.

> If I was hiring someone for you, if I pulled them from the ranks I would look for qualities of curiosity, curiosity would be a major quality, curiosity, determination. They want to get to the answer but also independence of thought; they don't necessarily go along with the crowd and I would want them to be pretty circumspect about things. I am not looking for the loner off in the corner who quietly . . . does his job but I'm also not looking for the office fly who is just constantly . . . circulating around the office yakking it up with his buddies. I am looking for someone in between, someone who's got a pretty solid analytical head on their shoulders, but they also talk to others. They are not intimidated by rank necessarily or position; they're looking at everything in a pretty cool-headed logical fashion but with an . . . awareness of, we are all political animals, we live in political organizations and . . . you have to follow the direction of the organization that you are working inside.[108]

[106] Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

[107] Ibid.

[108] Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

Other interviewees also stressed the need to look for the individual with curiosity, and imagination; one looks for the inveterate reader. They should be the kind of people that the department gives a problem to go at it with determination; they "love brainstorming all day," gnawing on the problem.[109] They should not be "boss fighters," but also not easily cowed by rank. Lastly, they need to be self-confident in that if they were working with outside analysts they would have to be comfortable working with people who are smarter than then they are on certain subject matter.[110] George Friedman recommended people who "love sitting at computer screens . . . and discerning patterns."[111]

The supervisor of this unit needs to be able to guide and be patient with these personality types. He or she also needs to be able to keep the unit on track, again determination, leadership, and the ability to get the best out of team members is required. Especially in the early stages, the supervisor is going to need to assure things are getting done. The department and possibly the municipal government will be watching to see what this unit is doing. It cannot be allowed to sit around thinking great thoughts; it needs to produce useful intelligence products.

> And the person that guides them doesn't necessarily have to be a professional analyst; it has to be just somebody interested in getting the mission done, a mission-oriented supervisor. And that person would say . . . , "Over the course of 90 days here, we're going to do something that has never been done before here within (this fire department). We're going to create an intelligence department to help us and to save our colleagues' lives. And the first thing we're going to look at is this. Now, how are we going to go about getting that done? And, oh, by the way, we need this done by, if this is a Monday, we need a completed project with your suggestions by Wednesday.[112]

[109] Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

[110] Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

[111] George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

[112] Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

So how might a department search for the right people? First off, open the unit up to all the personnel in a department whether they are uniformed members of the department, professional staff or civilians. The idea is to have as wide a pool of applicants as possible. One interviewee said, "I would solicit requests for an extremely bright individual with good writing skills with the ability to rapidly assess and process data. That person would need to take in not only the "granular and tactical data, but recognize the importance of strategic data."[113]

Have the individual write a paper on some homeland security topic that the department chooses and give them a very short time to do it. The short lead-time does two things. It shows that a person is motivated and that they are adaptable. Next, have the people the department has chosen work as a team. "I would give them projects to work on. And I would have them operate with very little direction and very guidance at first."[114] Again, this group is only going to be successful if they are self-motivated and adaptable.

How does a department know if the person they have placed into their intelligence unit is going to be successful? George Friedman reported that it would be known in 90 days if an individual were going to be a success in the intelligence unit. "He's going to start giving you smart stuff. He' going to tell you stuff you didn't know. Okay at first, he's only going to do it once or twice but a man that can give it to you once or twice can give you more. And if in 90 days he can't tell you anything you didn't know, he won't in 2000 (days)."[115] Therefore, a department should initially assign a member to an intelligence unit for a 90-day probationary period.

This chapter discusses the adaptability required by members of a fire department intelligence unit. Why should this be necessary? Many of those interviewed warned against "process" in analysis. In other words, having hard

[113] Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

[114] Ibid.

[115] George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

and fast rules about how do accomplish the tasks given to an intelligence unit is counterproductive. Mr. Johnson reported, "You know, from basic training on up you're kind of shoved inside a box and told to operate in there and with intelligence you just can't do that. If you box people in with too many rules, and regulations, and standards then you lose free expression, you lose freethinking and . . . innovative thinking. What was (what) they said after 9/11; the intelligence failure was one of imagination."[116] Get the intelligence team thinking differently, thinking analytically from a strategic and tactical perspective "not thinking regulation, not thinking process."[117]

Several of those interviewed stated that this lack of process might be uncomfortable for a local fire department; fire departments tend to be process driven organizations. However, as George Friedman stated about not having a predictable analytical process does indeed "sometimes creates chaos. But, better chaos than disciplined failure."[118]

So far, this chapter has discussed what to look for in a firefighter who is being considered for an analytical unit, but where does a fire department get a professional analyst to help in this effort? There are many ways. First, the department may be able to use grant money to hire an analyst. The analyst can mentor the firefighters coming into the unit. That way if the grant money runs out, the department already has a pool of trained members who can then mentor other firefighters. If this is not possible, look within the department for people who might have a military intelligence background. These individuals would not have to make a life-long commitment to the analysis unit. They could, instead, mentor other firefighters who were interested in this work. If the department is close to a military facility, talk to the commanding officer as there might be retired military intelligence people locally who might volunteer to help. Pat Miller, the Chief of Police in Ventura, California obtained analytical assistance this way. "I

[116] Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

[117] Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

[118] George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

knew there were retired Navy people around here so we went out to the base and the admiral gave us some names. And we called these guys and they were more than happy to help us out. They come in and (do) . . . mostly open source stuff but they still have clearances so they are still able to see stuff and they do a great job. They collect and write brief papers."[119]

The Association of Former Intelligence Officers (AFIO) is an educational organization of approximately 4,000 current and former intelligence professionals. The membership of the Association is spread across the United States. Leveraging the above idea, the Association was contacted by the researcher to see if they would be willing to act as a resource for fire departments that desired voluntary assistance in forming an intelligence unit. The Executive Director, Elizabeth Bancroft, graciously offered the assistance of the Association. If a fire department contacts her at (703) 790-0320, she will notify members of the Association who live in that area. If a local member of the Association is interested in helping, they can then contact the local fire department. Similarly, the Armed Forces Communications and Electronics Association (AFCEA International), an organization of 31,000, offered their assistance to fire departments that are beginning an intelligence unit. Their point of contact is Mr. Steven Ritchey, Vice President for Intelligence. Mr. Ritchey's phone number is (703) 631-613. His e-mail address is sritchey@afcea.org. If none of these resources is available in a particular locale, do without the intelligence professional; train personnel from within your department. If none of these resources is available in a particular locale, do without the intelligence professional; train personnel from within the department.

Balance is also required in an analytic unit. The smaller the group, the more critical it is to pick the right individuals. If only have three people . . . and all three are gregarious and outgoing then the unit is going to be known for, you know, these guys make all kinds of noise, they're always sending out memos,

[119] Pat Miller, interview by author, field notes, South Bend, Indiana, November 22, 2008.

this and that, but what the hell do they know? Or on the other hand, if you hire three guys who are studious and quiet, and you know shrinking violet types then, hello, did you hire anybody.[120] Since this thesis suggests a small group of individuals, these few people will create the unit's personality. It is important, then, not only to pick the individuals with the right mental abilities and writing skills, but also to pick the right balance of individuals.

3. Operations

What is the analytical unit supposed to do for a department? How should it be helping the local fire service organization prevent, respond to, and survive a terrorist attack? A lot of information and intelligence is available from federal agencies. Still, more is available from state and local fusion centers. The analytic unit or fire department intelligence officer looks at all of this incoming information and sees how it applies to the local fire department and the neighboring community. Additionally, the unit looks at the local community and asks how would terrorism affect a response to that building, to that factory, to that piece of infrastructure? It looks at a department's standard operating procedures and asks in light of what is known of terrorism, do they need to be changed, and is it possible to make members safer. The raison d'être of such a unit is to work for the safety of the members of a department, their fellow first responders, and the citizens of the community they serve.

"Every significant terrorist event is reported somewhere in the world."[121] Who is looking at these attacks, looking for the lessons learned, and asking what are the implications are for this department? "That's the way you learn, you go from hindsight to foresight."[122] The intelligence officer or unit attempts to predict

[120] Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

[121] George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

[122] John McCreary, interview by author, transcript, Washington, D.C., November 25, 2008.

the results if that attack happened in their community. Within larger communities, even different neighborhoods may face different threats. Fred Burton gave an example of how this local analysis might work.

> If I was trying to make this argument to the FDNY chief in New York and okay we know NYPD has this ring of steel in Wall Street or wherever it's deployed. What does that mean to me as (the department) responsible for emergency services in the area? Does this mean that thinking of this from an analytical perspective, now the bad guys won't look at this area; therefore, where would they go? Where are the other softer target areas that perhaps I need to be made aware of? In the event we do have a call for service in this "ring of steel," do I automatically dispatch . . . a full box alarm assignment versus just a first due engine company? I mean these are the kinds of things that an analytic shop could game board and give you some potential options or some alternative analysis as to other things you should be thinking of.[123]

Additionally, the analysis unit should be the people who answer the phone when field companies or EMS units discover things they consider suspicious and need to ask questions. They should be looking at reports. A department needs somebody who is really looking at terrorism around the world to answer phones or correlate reports.[124]

This unit needs to ask the tough questions of a department, are they prepared? The intelligence unit, possibly in conjunction with the area's police department and local Protective Security Advisor should make of a list of potential terrorist targets. Look at the top 50 potential targets; it is not an insurmountable number.[125] The unit looks at the current fire department response and asks if there were a terrorist attack on this target, how would the response need to change? Where would water be obtained? How would members and the public be protected? What if there were multiple attacks, how

[123] Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

[124] George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

[125] John McCreary, interview by author, field notes, Washington, D.C., November 25, 2008.

would resources be obtained? This is not new; fire departments have been doing target hazard planning for years, this unit does the same thing except though the lens of terrorism.

The analytic unit needs to look at a community through the eyes of a terrorist. Often, homeland security analysts look at vulnerabilities. Exploring vulnerabilities may not be the best way to discover potential targets for response planning. Just because a potential infrastructure target is vulnerable does not mean a terrorist is interested in it. "What do they like to attack? They go for sensational targets – headlines – not for fundamental and revolutionary change. If it is possible to see through terrorist eyes at what they would like to attack if they had their druthers, one would find it does not look like the list of vulnerable targets that law abiding analysts identify."[126] Therefore, another way to look at potential targets is through the use of attractors. "Because that is the only relevant starting point. What do they (the terrorists) see as viable, an attractive target? So, we developed . . . a set of attractors."[127] "We used 36 of the most sensational attacks in the world to come up with this alternative" to critical infrastructure vulnerabilities.[128] The attractors this research found were the following.

- Visibility – sensational press
- Essentiality – lack of workarounds
- Occupied -- lots of people
- Accessibility – easy to get to
- Inter related – Multiple effects and big bang for the buck
- Symbolism – psychological impact[129]

This list assists in looking at targeting from the eyes of an adversary; fire department analysts need to do the same thing.

[126] John McCreary, e-mail message to author, November 23, 2008.

[127] John McCreary, interview by author, transcript, Washington, D.C., November 25, 2008.

[128] Ibid.

[129] John McCreary, "The Critical Infrastructure Warning Project," Booz Allen Hamilton, 2003.

In summary, analysis is performed by a small group of dedicated and mentally flexible individuals, three to four at most.[130] "You 'right size' it (the analytical unit) by asking the question how do I make certain that everything I receive . . . is seen by a small enough group that they can collate it." Bigger is not better. It is better to have two people who know all the facts than ten people who each know one fact. In any event, this unit should have a steady supply of information coming in, and analyze it to see how or if it applies to the local community. These units should look at attacks around the world for lessons that can be used by the local fire department. They should look at potential targets in the community and plan a fire department's response; they should be available to answer questions from field units and make contacts with other agencies in the area that are involved with homeland security. Analysis should support preparedness and pre-planning in a department.[131] Ultimately, by their research and planning, they protect life and property in their local community.

E. DISSEMINATION

1. Information Transfer

The method of dissemination is the one place in the intelligence cycle for a fire department's intelligence shop not to be imaginative. Almost all of those interviewed recommended that an intelligence office act through existing processes. This is especially true as an intelligence office comes on line; later the office may tweak the system, but it is initially easier to go through existing communication pathways. Mark Johnson stated, "So I would try to do it through the existing (communications processes), you don't want to necessarily set up a brand new information sharing process. That may or may not be advisable depending on the situation but in general, most organizations, mature

[130] George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

[131] "Fire Department Intelligence Officer," *FDSOA Safety-Gram* 15 (February 2007): 1.

organizations . . . already have their set way of doing things and trying to change it is sometimes not pretty."[132] In other words, do not make waves where waves are not necessary. Use the communication pathways that already exist.

A fire department intelligence unit needs to be discreet. Not all information should be sent to all members of the department. The intelligence unit will need to decide what intelligence is useful for the higher echelons of the department and what should go to the field companies. Intelligence that affects situational awareness should be sent to all levels of the department. In the Ventura Police Department, "we leave it to that (TLO) sergeant to decide if they are going to put that out to the troops or do a training bulletin or do some kind of notice or something that uh he feels or she feels is would be valuable for the street officer and then do through briefings you know roll calls and things like that."[133]

George Friedman recommends that the intelligence unit have "a method for disseminating it (intelligence) not only to the fire department but to the police department as well so that they can be alerted."[134] It is also important to pass the information along to other parts of the department other than the field units. For instance, fire inspectors should be included because they are in various premises and are potentially valuable sources of additional information, if they know what they are seeking. Another division of the department that should be included in the information flow is training. Correct and up to date information should appear in training scenarios and training bulletins. Though discreet, dissemination should be as wide ranging as is necessary for the intelligence unit to fulfill its duty to protect life and property.

[132] Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

[133] Pat Miller, interview by author, transcript, South Bend, Indiana, November 22, 2008.

[134] George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

2. Feedback

Along with the written materials, the intelligence unit is disseminating some type of feedback form that should be included. It does not matter if the dissemination is electronic or paper, the consumer should have a chance to give comments on the materials received. This is a form of quality control. Remember the whole point of this intelligence process is to support the consumer of the product. If there is no feedback process, an intelligence unit until never improve the products it is putting out. "For each article that we (the Open Source Center) put up on our web site anyone reading that can respond and ask a question, make a statement, whatever and once they hit the send button it comes to our customer service team who are not the experts but they will immediately pass it off to the author or someone else who knows about the subject matter."[135] An intelligence unit should not be afraid to ask if their materials were useful or how they could be improved.

Moreover, the feedback process allows consumers of intelligence to ask questions on the materials presented. One of the purposes of an intelligence unit is to educate the department they serve. Any request for additional information on the materials disseminated should be welcomed and be given a rapid response. If an intelligence unit does not have the information at hand, so inform the consumer right away. Then try to find the information requested. Being responsive earns a lot of good will for the intelligence unit.

Part of the feedback process is also to ask the department's senior managers and its firefighters what they feel they need to know. What information, what intelligence in their mind is lacking? Leave a space on the feedback form asking what the consumer would want to know about or feel is lacking in their understanding of terrorism. Bear in mind, the intelligence cycle is a cycle; the process is iterative. The issues department personnel want or need

[135] Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

to know about are really nothing other than new requirements. Requirements are, of course, the first step of the intelligence cycle. These new requirements cause a new cycle of collection and the process continues.

IV. RECOMMENDATIONS

A. TRAINING

Every person interviewed stressed the need for firefighters in the intelligence unit to be properly trained. The interviewees may not have all agreed on how best to train a firefighter; howbeit, training was stressed as one of the most important factors in the success of a fire department intelligence project. The methodologies ranged from mentoring to formal classroom training. Formal training can come from government or from academia, whereas mentors may be volunteers with an intelligence background coming out of the local community or a vendor hired for a limited period. Again, a department should not forget to see if they have personnel with a military intelligence background who might be willing to assist in the effort.

1. Formal Instruction

One good resource for training is the Open Source Center outside of Washington, D.C. Mark Johnson of the Open Source Center reported, "We offer training and we have a whole catalog of courses and perhaps a dozen of them are relevant to a person like at a fire department. We teach analytical, basic analytical methods and advanced analytical methods."[136] The courses themselves are free of charge. The local fire department pays associated travel costs.

Also at the federal level, the Department of Homeland Security's Office of Intelligence and Analysis offers training. The DHS "Intelligence Training Branch . . . has begun to develop homeland security-centric courses for our DHS intelligence personnel and our state, local and tribal partners at our own

[136] Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

Homeland Security Intelligence Training Center in Ashburn, Va."[137] The Basic Intelligence and Threat Analysis Course (BITAC) is a five-week course that awards a Homeland Security Intelligence Officer designation. Fire department personnel may take these courses at no cost and grant money may be provided to cover travel costs.

There may also be training available at a state or local level. For instance, the Department of Homeland Security offers courses in open source intelligence through the State and Fusion Center Program office.[138] These programs provide training in open source tradecraft. "We call it tradecraft, it's how to analyze, how to evaluate sources, it's basically teaching you common sense methods in understanding the information coming at you and separating the fluff from the real, (find) the good stuff and then taking all those bits of information, laying them out on the table and then writing, describing what it is you are reading there, what are you seeing there and are there any judgments to be gained from that, and . . . where to get information."[139] Some states may have a Terrorist Liaison Officer program available. Pat Miller recommended that departments "train some firefighters as Terrorist Liaison Officers" as a good way to start an intelligence program.[140]

In addition, there are university programs that train people in intelligence. Mark Johnson stated,

> There are a number of universities and colleges that have established intelligence educational curriculum. One that stands out in my mind is Michigan State University, Dr. Dave Carter, he teaches constantly. He is constantly on the road at police departments nationwide teaching open source methods, intelligence methods. He wrote papers on intelligence . . . these

[137] Charles Allen, "The Department Develops its Own Professional Intelligence Workforce," *Leadership Journal*, January 14, 2009. http://www.dhs.gov/journal/leadership/labels/Intelligence%20and%20Analysis%20Directorate.html (accessed February 7, 2009).

[138] Mark Johnson, interview by author, field notes, Washington, D.C., November 4, 2008.

[139] Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

[140] Pat Miller, interview by author, transcript, South Bend, Indiana, November 22, 2008.

> sorts of topics. So (you have the) Open Source Center at the federal level and then you got a few colleges and universities, Michigan State, I think Penn State has some, New Mexico, I heard about an intelligence program up there.[141]

There are also formal on-line training programs available. Fred Burton pointed out that the Bush School at Texas A&M has an on-line Homeland Security Department.[142] Henley-Putnam University is accredited and is highly recommended.

> Henley-Putnam has got the best tactical training courses that I have ever seen in an online format. And the FBI (and), for example, all the agents assigned as ATF analysts, have recognized this program as (the) one. If (FBI agents) want to take the courses there online, the FBI will pay for it. And, I mean they have (relevant) courses, courses, you know, not like English 101 or Writing 101. They have . . . Surveillance Detection Training . . . Strategic Analysis, Tactical Analysis courses, How Do You Do a Threat Assessment. And so, they've got some very good courses that also come with very good instructors and very good training manuals that, you know, and books and so forth that you get to refer back to.[143]

These types of programs are of great benefit in a busy world because fire department members can take courses in analysis in an on-line format.

2. Mentoring

Several of those interviewed recommended mentoring as the best way of training fire department members as analysts. The idea would be that fire personnel would become a good analyst by working directly with and learning from a good analysts. George Friedman suggested, "The best way to train these guys is to attach them to an analyst doing work and make them his assistant for three months. You know go get me coffee, go Xerox this, go check this fact out, go check that fact out. And then you see it's really a master craftsman working

[141] Mark Johnson, interview by author, transcript, Washington, D.C., November 4, 2008.

[142] Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

[143] Ibid.

as apprentice. And in due course he becomes quite good."[144] Some successful private intelligence agencies train their new analysts in this fashion; they believe mentoring is superior to formal training because their new analysts learn to avoid the restrictive hard and fast rules of the American intelligence community.[145]

There are several ways a mentoring program could be initiated by a department. As was written earlier, a department may have internal resources such as former military intelligence veterans who might mentor personnel in an intelligence unit. The first step, then, is to check within one's own department. The next step is to check one's community. Are there military facilities that might help put a department in touch with retired intelligence officers? Lastly, as mentioned previously, several intelligence associations have offered to set-up an intelligence mentor with a local fire department.

B. KEEPING IT REAL

Many of the interviewees stressed the need for a new analysis unit to "keep it real." Though this was mentioned before, it is worth repeating, the intelligence produced by the new unit must be related to the operations of that department. It has to have clear value. If city or department administrators are to support this project, they must see real value. Real value comes from the analysis unit improving their department. If the intelligence produced is not actionable, the unit will loose support. "Write what the department needs. You might do great writing, but it's not on a topic that anyone needs it is worthless."[146] Similarly, John McCreary commented on the intelligence generated by a fire department intelligence unit, "There is real value to this if there is information that is relevant to your mission."[147]

[144] George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

[145] Ibid.

[146] Ibid.

[147] John McCreary, interview by author, transcript, Washington, D.C., November 25, 2008.

Look at areas in the department that have a potential to fail in the event of a terrorist attack, work at improving those areas. Do the homework. If it is not known, then admit as such. Do not make up answers. "Credibility is golden, if you don't know, say so. Try to find the answers."[148] Once an intelligence unit's credibility is gone, it is dead in the water. Chances are it will never get its credibility back.

If an intelligence unit does good analysis and writing, it will be noticed. "When your intelligence department writes something that probably would be unusual, but in many ways brilliant, the battalion chief when he reads that report . . . is going to say, 'Wow. I want more of that.' And word of mouth itself would grow that section (analysis unit)."[149] Keep the unit's research real, keep it relevant, and keep it credible. If a department is going to form an intelligence unit or even if it is only one intelligence officer, Fred Burton summarized the mandate of this initial phase of the project well, when he said, "You have a limited window to impress. Don't waste it."[150]

[148] George Friedman, interview by author, transcript, Austin, Texas, November 19, 2008.

[149] Fred Burton, interview by author, transcript, Austin, Texas, November 25, 2008.

[150] Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS

A. PROPOSITIONAL MODEL

The research shows there are definitive relationships between the Aggregated Second Order Codes. First, the entire fire intelligence process must be surrounded with integrity and usefulness. These are the same values that govern the fire service on a day-to-day basis. These mandatory overarching values will keep the intelligence unit in operation and supported by their department. This second order code is called “Keeping it Real” and it encircles all others. Within that context, intelligence must be understood as a process and all the other aspects of the research are, therefore, contained within the second order code “Intelligence.” The process begins with “Requirements.” Someone or some committee must decide what a department needs to know. Some interviewees recommended against a formal requirement system and argued to allow the analysts themselves to decide what a department needs to know. Howbeit, some individual or group of individuals must make that determination and that is “Requirements.”

From the requirements, the intelligence unit begins to bring together the requisite information and intelligence; this second order code is called “Collection.” The collected materials then undergo “Analysis.” The analytical process is where an intelligence unit asks, among other questions, what does this fact or event mean to this particular fire department. How will it affect operations? Will it endanger citizens, firefighters, fellow first responders? The analytical product is then sent out to those who need the information it contains. This process comes under the second order code “Dissemination.” Part of the dissemination process is the allowance for feedback from the consumer. The questions contained in the feedback may lead to new requirements. “Training” improves the ability of the intelligence to recognize a department’s requirements. Additionally, good training improves collection and analysis by the intelligence unit.

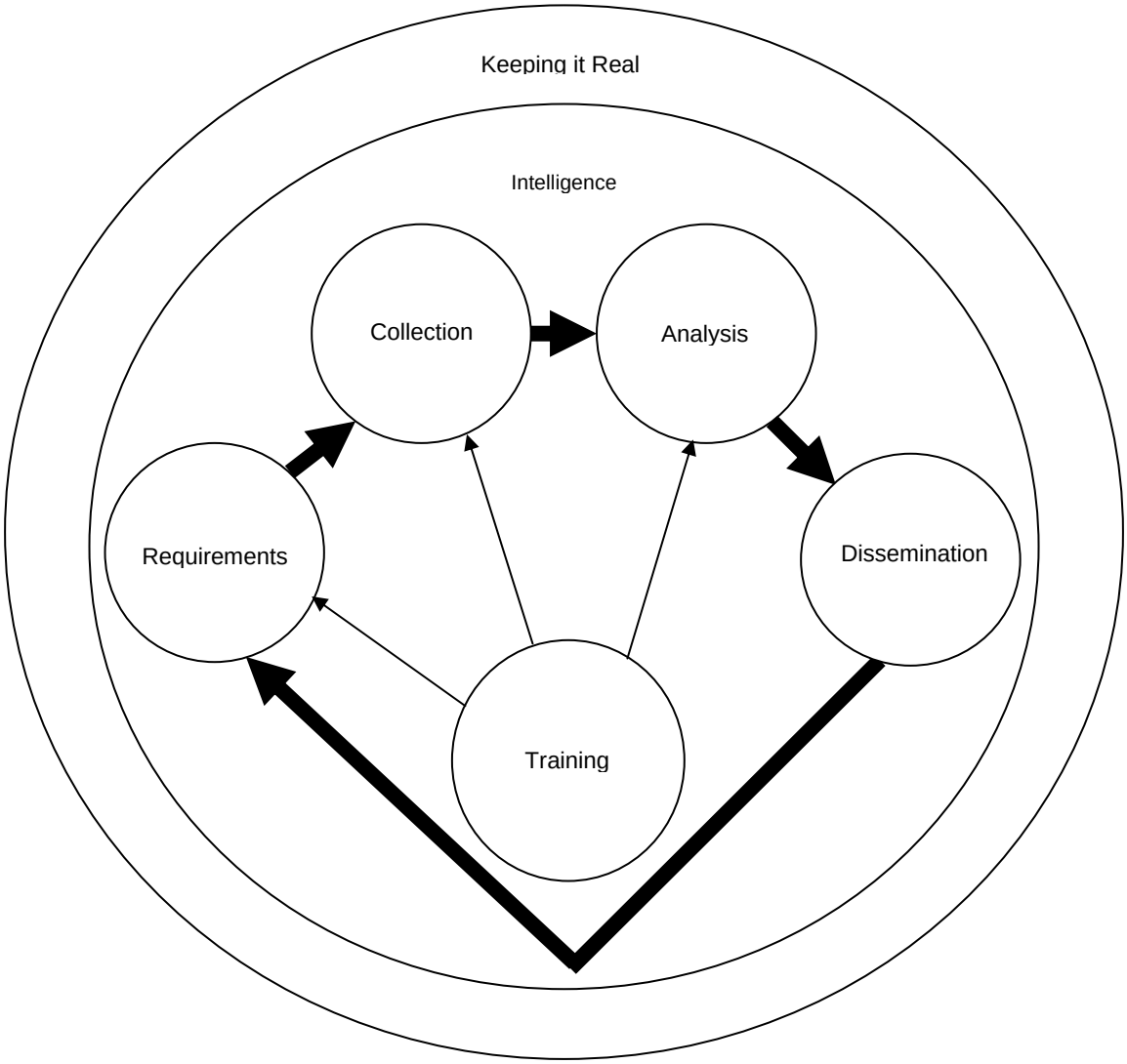


Figure 3. Propositional Model

B. INTELLIGENCE IN THE FIRE SERVICE

Those interviewed in this study clearly understood the need for fire departments to have their own intelligence officers or units. Everyone involved in this project was eager to help the fire service develop the skills and systems necessary to execute this vital work because they saw that need. No one, not the fusion center, not the local police, not federal agency can understand what a piece of intelligence means to a particular fire department with a particular set of procedures in a particular locale. Only the local firefighter has that wisdom. For

that reason, every fire department should have personnel trained in intelligence and informing their department on terrorism. This is not just the conclusion of this research. The Fire Department Safety Officers Association (FDSOA) also recommends that every department have an intelligence officer.[151] Terrorism threatens both the lives of the citizens a department is sworn to protect and the firefighters themselves. Protecting life and property is the reason a fire department exists. An intelligence officer or unit helps a department fulfill that sworn duty.

[151] "Fire Department Intelligence Officer," *FDSOA Safety-Gram* 15 (February 2007): 2.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Allen, Charles. "The Department Develops its Own Professional Intelligence Workforce." *Leadership Journal*, January 14, 2009, http://www.dhs.gov/journal/leadership/labels/Intelligence%20and%20Analysis%20Directorate.html (accessed February 7, 2009).

Benavides, Ben. U.S. Army Intelligence Center. *Targeting Tomorrow's Terrorist Today (T^4) through Open Source Intelligence (OSINT): Quick-Links Starter Handbook for the Open Source Analyst*. Fort Huachuca, January 2007.

Blatus, Richard J. *Altering the Mission Statement: The Training of Firefighters as Intelligence Gatherers*. Master's Thesis, Naval Postgraduate School, 2008.

Bush, George. *Executive Order 13356: Further Strengthening the Sharing of Terrorism Information to Protect America*. Washington, D.C., The White House, October 25, 2005. http://www.whitehouse.gov/news/releases/2005/10/print/20051025-5.html (accessed July 11, 2008).

Calder, Rich and Murray Weiss. "Stash 'Bagged' at Market." *New York Post*, April 27, 2005.

Cloud, Rosemary. *Future Role of Fire Service in Homeland Security*. Master's Thesis, Naval Postgraduate School, 2008.

Corbin, Juliet and Anselm Strauss. *Basics of Qualitative Research*. 3rd ed. Sage Publications, Thousand Oaks, CA, 2008.

Dabruzzi, Kyle and Daveed Gartenstein-Ross. "Firefighters' Developing Role in Counter Terrorism." *Policing Terrorism Report* 3 (July 2008).

"Fire Department Intelligence Officer." *FDSOA Safety-Gram* 15 (February 2007): 1-4.

Fire Department, City of New York (FDNY). *FDNY-DHS Intelligence Enterprise: Phase II Work Plan 01 April 2007 – 01 October 2007*. New York, March 2007.

Fire Department, City of New York (FDNY). *Terrorism and Disaster Preparedness Strategy*. New York, 2007.

Fire Service Intelligence Enterprise. *Progress Report 1*. December 28, 2007.

Heuer, Richards J. *Psychology of Intelligence Analysis*. Washington, D.C., Center for the Study of Intelligence, 1999.

Jardines, Eliot A. Office of the Director of National Intelligence. *National Open Source Enterprise*. Washington, D.C., April 2006.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. 3rd ed. Washington, D.C.: CQ Press, 2006.

North Atlantic Treaty Organization. *NATO Open Source Intelligence Reader*. February 2002.

North Atlantic Treaty Organization. *NATO Open Source Intelligence Handbook*. November 2001.

Rubin, Herbert J. and Irene, S. Rubin. *Qualitative Interviewing: The Art of Hearing Data*. 2nd ed., Sage Publications, Thousand Oaks, CA, 2005.

Sims, Jennifer, and Burton Gerber, eds., *Transforming U.S. Intelligence*. Washington, D.C.: Georgetown University Press, 2005.

Stalder, Felix, and Jesse Hirsh. "Open Source Intelligence." *First Monday*, 7, no. 6 (June 2002), http://www.noemalab.org/sections/ideas/ideas_articles/pdf/stadler_hirsh_opensource.pdf (accessed April 18, 2008).

Steele, Robert David. *Open Source Intelligence: Executive Overview*. Global Intelligence Partnership Network, January 1, 2004. http://www.oss.net/, (accessed April 18, 2008).

Thomas, Gail Fann. "Research Methods: Qualitative Data Analysis." https://www.chds.us/courses/file.php/279/lecture_transcript/6-res_methods_qual_datas_analysis_transcript.doc?forcedownload=1 (accessed January 22, 2009).

U.S. Congress. House of Representatives. Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security. *Using Open Source Information Effectively*. 109th Cong., 1st sess., June 21, 2005.

U.S. Congress. Senate. Select Committee on Intelligence. *Intelligence Reform and Homeland Security Intelligence*. 110th Cong. 1st sess., 2007.

U.S. Congressional Research Service. CRS Report for Congress. *Open Source Intelligence (OSINT): Issues for Congress*. Washington, D.C., updated January 28, 2008.

U.S. Department of Justice. Bureau of Justice Assistance. *Intelligence-Led Policing: The New Intelligence Architecture*. Washington, D.C., September 2005. http://www.ncjrs.gov/pdff.lesl/bja/210681.pdf (accessed July 7, 2008.

U.S. Department of Justice. Bureau of Justice Assistance. *The National Criminal Intelligence Plan*. Washington, D.C., June 2005. http://www.it.ojp.gov/documents/National_Criminal_Intelligence_Sharing_Plan.pdf (accessed July 10, 2008).

U.S. Department of Homeland Security. Lessons Learned Information Sharing. *LLIS Intelligence and Information Sharing Initiative: Homeland Security Intelligence Requirements Process*. December 2005.

U.S. Department of Homeland Security. Office of Intelligence and Analysis. *Open Source for Fusion Center Practitioners*. n.d.

U.S. Department of the Army. *Open Source Intelligence FMI 2-22.9*. Washington, D.C., December 5, 2006.

Weeks, Douglas M. *Strategic Changes for the Fire Service in the Post-9/11 Era*. Master's Thesis, Naval Postgraduate School, 2007.

Werner, Charles. "Progress Report: Information, Intelligence for the Fire Service." *Firehouse* 29 (December 2004): 40-42.

Wilson, Michael R. "Intelligence Units Reduce Arson." *Fire Chief* 32 (August 1988): 46-49.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
 Ft. Belvoir, Virginia

2. Dudley Knox Library
 Naval Postgraduate School
 Monterey, California

3. Chief of Department Salvatore Cassano
 Fire Department, City of New York
 Brooklyn, New York

4. Assistant Chief Joseph Pfeifer
 Fire Department, City of New York
 Brooklyn, New York

FM 2-22.3 (FM 34-52)

HUMAN INTELLIGENCE COLLECTOR OPERATIONS

HEADQUARTERS, DEPARTMENT OF THE ARMY

September 2006

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

NOTE: All previous versions of this manual are obsolete. This document is identical in content to the version dated 6 September 2006. All previous versions of this manual should be destroyed in accordance with appropriate Army policies and regulations.

This publication is available at
Army Knowledge Online (www.us.army.mil) and
General Dennis J. Reimer Training and Doctrine
Digital Library at (www.train.army.mil).

Field Manual
No. 2-22.3

*FM 2-22.3 (FM 34-52)
Headquarters
Department of the Army
Washington, DC, 6 September 2006

Human Intelligence Collector Operations

Contents

		Page
	PREFACE	vi
PART ONE	**HUMINT SUPPORT, PLANNING, AND MANAGEMENT**	
Chapter 1	**INTRODUCTION**	1-1
	Intelligence Battlefield Operating System	1-1
	Intelligence Process	1-1
	Human Intelligence	1-4
	HUMINT Source	1-4
	HUMINT Collection and Related Activities	1-7
	Traits of a HUMINT Collector	1-10
	Required Areas of Knowledge	1-12
	Capabilities and Limitations	1-13
Chapter 2	**HUMAN INTELLIGENCE STRUCTURE**	2-1
	Organization and Structure	2-1
	HUMINT Control Organizations	2-2
	HUMINT Analysis and Production Organizations	2-6

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

NOTE: All previous versions of this manual are obsolete. This document is identical in content to the version dated 6 September 2006. All previous versions of this manual should be destroyed in accordance with appropriate Army policies and regulations.

*This publication supersedes FM 34-52, 28 September 1992, and ST 2-22.7, Tactical Human Intelligence and Counterintelligence Operations, April 2002.

Chapter 3 **HUMINT IN SUPPORT OF ARMY OPERATIONS** 3-1
Offensive Operations 3-1
Defensive Operations 3-2
Stability and Reconstruction Operations 3-3
Civil Support Operations 3-7
Military Operations in Urban Environment 3-8
HUMINT Collection Environments 3-8
EAC HUMINT 3-9
Joint, Combined, and DOD HUMINT Organizations 3-10

Chapter 4 **HUMINT OPERATIONS PLANNING AND MANAGEMENT** 4-1
HUMINT and the Operations Process 4-1
HUMINT Command and Control 4-3
Technical Control 4-4
Command and Support Relationships 4-4
HUMINT Requirements Management 4-5
HUMINT Mission Planning 4-15
Task Organization 4-18
Operational Considerations 4-19
Operations Plans, Operations Orders, and Annexes 4-21
Operational Coordination 4-22

PART TWO **HUMINT COLLECTION IN MILITARY SOURCE OPERATIONS**

Chapter 5 **HUMINT COLLECTION** 5-1
HUMINT Collection Operations 5-1
Human Source Contact Operations 5-2
Debriefing Operations 5-7
Liaison Operations 5-12
Interrogation Operations 5-13
Types of Interrogation Operations 5-27

PART THREE **THE HUMINT COLLECTION PROCESS**

Chapter 6 **SCREENING** 6-1
Human Source Screening 6-1
Screening Operations 6-2
Screening Process 6-9
Screening Methodologies 6-11
Screening Requirements 6-12

Initial Data and Observations 6-13
Source Assessment 6-14
Other Types of Screening Operations 6-15

Chapter 7 PLANNING AND PREPARATION 7-1
Collection Objectives 7-1
Research 7-1
HUMINT Collection Plan 7-8
Final Preparations 7-13

Chapter 8 APPROACH TECHNIQUES AND TERMINATION STRATEGIES 8-1
Approach Phase 8-1
Developing Rapport 8-3
Approach Techniques 8-6
Approach Strategies for Interrogation 8-20
Approach Strategies for Debriefing 8-21
Approach Strategies for Elicitation 8-22
Termination Phase 8-23

Chapter 9 QUESTIONING 9-1
General Questioning Principles 9-1
Direct Questions 9-1
Elicitation 9-5
Leads 9-5
Detecting Deceit 9-6
HUMINT Collection Aids 9-9
Recording Techniques 9-9
Questioning With an Analyst or a Technical Expert 9-11
Third-Party Official and Hearsay Information 9-12
Conducting Map Tracking 9-13
Special Source Categories 9-16

Chapter 10 REPORTING 10-1
Reporting Principles 10-1
Report Types 10-1
Reporting Architecture 10-5

Chapter 11 **HUMINT COLLECTION WITH AN INTERPRETER** 11-1
Advantages and Disadvantages of Interpreter Use 11-1
Methods of Interpreter Use 11-2
Sources of Interpreters 11-4
Interpretation Techniques 11-5
Training and Briefing the Interpreter 11-5
Placement of the Interpreter 11-6
Interactions With and Correction of the Interpreter 11-7
Interpreter Support in Report Writing 11-8
Evaluating the Interpreter 11-8
Managing an Interpreter Program 11-9

PART FOUR **ANALYSIS AND TOOLS**

Chapter 12 **HUMINT ANALYSIS AND PRODUCTION** 12-1
Analytical Support to Operational Planning 12-1
Operational Analysis and Assessment 12-3
Source Analysis 12-4
Single-Discipline HUMINT Analysis and Production 12-4
HUMINT Source Selection 12-19

Chapter 13 **AUTOMATION AND COMMUNICATION** 13-1
Automation 13-1
Collection Support Automation Requirements 13-2
Analytical Automation Requirements 13-3
Automation Systems 13-7
Communications 13-8

APPENDIX A **GENEVA CONVENTIONS** A-1
Section I. Geneva Conventions Relative to the Treatment of Prisoners of War (Third Geneva Convention) A-1
Section II. Geneva Conventions Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention) A-47

APPENDIX B **SOURCE AND INFORMATION RELIABILITY MATRIX** B-1

APPENDIX C **PRE-DEPLOYMENT PLANNING** C-1

APPENDIX D **S2 GUIDE FOR HANDLING DETAINEES, CAPTURED ENEMY DOCUMENTS, AND CAPTURED ENEMY EQUIPMENT** D-1

APPENDIX E **EXTRACTS FROM ALLIED JOINT PUBLICATION (AJP)-2.5** E-1

APPENDIX F **NATO SYSTEM OF ALLOCATING INTERROGATION SERIAL NUMBERS** ... F-1

APPENDIX G **QUESTIONING QUICK REFERENCE** G-1

APPENDIX H **SALUTE REPORTING** H-1

APPENDIX I **DOCUMENT EXPLOITATION AND HANDLING** I-1

APPENDIX J **REFERENCES** J-1

APPENDIX K **CONTRACT INTERROGATORS** K-1

APPENDIX L **SAMPLE EQUIPMENT FOR HCT OPERATIONS** L-1

APPENDIX M **RESTRICTED INTERROGATION TECHNIQUE - SEPARATION** M-1

GLOSSARY Glossary-1

BIBLIOGRAPHY Bibliography-1

INDEX Index-1

Preface

This manual provides doctrinal guidance, techniques, and procedures governing the employment of human intelligence (HUMINT) collection and analytical assets in support of the commander's intelligence needs. It outlines—

- HUMINT operations.
- The HUMINT collector's role within the intelligence operating system.
- The roles and responsibilities of the HUMINT collectors and the roles of those providing the command, control, and technical support of HUMINT collection operations.

This manual expands upon the information contained in FM 2-0. It supersedes FM 34-52 and rescinds ST 2-22.7. It is consistent with doctrine in FM 3-0, FM 5-0, FM 6-0, and JP 2-0. In accordance with the Detainee Treatment Act of 2005, the only interrogation approaches and techniques that are authorized for use against any detainee, regardless of status or characterization, are those authorized and listed in this Field Manual. Some of the approaches and techniques authorized and listed in this Field Manual also require additional specified approval before implementation.

This manual will be reviewed annually and may be amended or updated from time to time to account for changes in doctrine, policy, or law, and to address lessons learned.

This manual provides the doctrinal guidance for HUMINT collectors and commanders and staffs of the MI organizations responsible for planning and executing HUMINT operations. This manual also serves as a reference for personnel developing doctrine, tactics, techniques, and procedures (TTP); materiel and force structure; institutional and unit training; and standing operating procedures (SOPs), for HUMINT operations at all army echelons. In accordance with TRADOC Regulation 25-36, the doctrine in this field manual is not policy (in and of itself), but is "…a body of thought on how Army forces operate….[It] provides an authoritative guide for leaders and soldiers, while allowing freedom to adapt to circumstances."

This manual applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the United States Army Reserve unless otherwise stated. This manual also applies to DOD civilian employees and contractors with responsibility to engage in HUMINT collection activities. It is also intended for commanders and staffs of joint and combined commands, and Service Component Commands (SCC). Although this is Army doctrine, adaptations will have to be made by other Military Departments, based on each of their organizations and specific doctrine.

Material in this manual applies to the full range of military operations. Principles outlined also are valid under conditions involving use of electronic warfare (EW) or nuclear, biological, or chemical (NBC) weapons.

This manual is intended for use by military, civilian, and civilian contractor HUMINT collectors, as well as commanders, staff officers, and military intelligence (MI) personnel charged with the responsibility of the HUMINT collection effort.

HUMINT operations vary depending on the source of the information. It is essential that all HUMINT collectors understand that, whereas operations and sources may

differ, the handling and treatment of sources must be accomplished in accordance with applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including fragmentary orders (FRAGOs).

Interrogation, the HUMINT subdiscipline responsible for MI exploitation of enemy personnel and their documents to answer the supported specific information requirements (SIRs), requires the HUMINT collector to be fully familiar with both the classification of the source and applicable law. The principles and techniques of HUMINT collection are to be used within the constraints established by US law including the following:

- The Uniform Code of Military Justice (UCMJ).
- Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (including Common Article III), August 12, 1949; hereinafter referred to as GWS.
- Geneva Convention Relative to the Treatment of Prisoners of War (including Common Article III), August 12, 1949; hereinafter referred to as GPW.
- Geneva Convention Relative to the Protection of Civilian Persons in Time of War (including Common Article III), August 12, 1949; hereinafter referred to as GC.
- Detainee Treatment Act of 2005, Public Law No. 109-163, Title XIV.

HUMINT collectors must understand specific terms used to identify categories of personnel when referring to the principles and techniques of interrogation. Determination of a detainee's status may take a significant time and may not be completed until well after the time of capture. Therefore, there will be no difference in the treatment of a detainee of any status from the moment of capture until such a determination is made. The following terms are presented here and in the glossary.

- Civilian Internee: A person detained or interned in the United States or in occupied territory for security reasons, or for protection, or because he or she has committed an offense against the detaining power, and who is entitled to "protected person" status under the GC.
- Enemy Prisoner of War (EPW): A detained person, as defined in Articles 4 and 5 of the GPW. In particular, one who, while engaged in combat under orders of his or her government, is captured by the armed forces of the enemy. As such, he or she is entitled to the combatant's privilege of immunity from the municipal law of the capturing state for warlike acts that do not amount to breaches of the law of armed conflict. For example, an EPW may be, but is not limited to, any person belonging to one of the following categories of personnel who have fallen into the power of the enemy; a member of the armed forces, organized militia or volunteer corps; a person who accompanies the armed forces, without actually being a member thereof; a member of a merchant marine or civilian aircraft crew not qualifying for more favorable treatment; or individuals who, on the approach of the enemy, spontaneously take up arms to resist invading forces.
- Other Detainees: Persons in the custody of the US Armed Forces who have not been classified as an EPW (Article 4, GPW), retained personnel (Article 33, GPW), and Civilian Internee (Articles 27, 41, 48, and 78, GC) shall be treated as EPWs until a legal status is ascertained by competent authority; for example, by Article 5 Tribunal.
- Retained Personnel: (See Articles 24 and 26, GWS.)

 - Official medical personnel of the armed forces exclusively engaged in the search for, or the collection, transport or treatment of wounded or sick, or in the prevention of disease, and staff exclusively engaged in the administration of medical units and facilities.
 - Chaplains attached to the armed forces.
 - Staff of National Red Cross Societies and that of other Volunteer Aid Societies, duly recognized and authorized by their governments to assist Medical Service personnel of their own armed forces, provided they are exclusively engaged in the search for, or the collection, transport or treatment of wounded or sick, or in the prevention of disease, and provided that the staff of such societies are subject to military laws and regulations.

- Protected Persons: Include civilians entitled to protection under the GC, including those we retain in the course of a conflict, no matter what the reason.
- Enemy Combatant: In general, a person engaged in hostilities against the United States or its coalition partners during an armed conflict. The term "enemy combatant" includes both "lawful enemy combatants" and "unlawful enemy combatants." All captured or detained personnel, regardless of status, shall be treated humanely, and in accordance with the Detainee Treatment Act of 2005 and DOD Directive 2310.1E, "Department of Defense Detainee Program", and no person in the custody or under the control of DOD, regardless of nationality or physical location, shall be subject to torture or cruel, inhuman, or degrading treatment or punishment, in accordance with and as defined in US law.
 - **Lawful Enemy Combatant:** Lawful enemy combatants, who are entitled to protections under the Geneva Conventions, include members of the regular armed forces of a State Party to the conflict; militia, volunteer corps, and organized resistance movements belonging to a State Party to the conflict, which are under responsible command, wear a fixed distinctive sign recognizable at a distance, carry their arms openly, and abide by the laws of war; and members of regular armed forces who profess allegiance to a government or an authority not recognized by the detaining power.
 - **Unlawful Enemy Combatant:** Unlawful enemy combatants are persons not entitled to combatant immunity, who engage in acts against the United States or its coalition partners in violation of the laws and customs of war during an armed conflict. For the purposes of the war on terrorism, the term "unlawful enemy combatant" is defined to include, but is not limited to, an individual who is or was part of or supporting Taliban or al Qaeda forces, or associated forces that are engaged in hostilities against the United States or its coalition partners.

Headquarters, U.S. Army Training and Doctrine Command (TRADOC) is the proponent for this publication. The preparing agency is the US Army Intelligence Center and Fort Huachuca, Fort Huachuca, AZ. Send written comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commander, ATZS-CDI-D (FM 2-22.3), U.S. Army Intelligence Center and Fort Huachuca, 550 Cibeque Street, Fort Huachuca, AZ 85613-7017. Send comments and recommendations by e-mail to ATZS-FDT-D@hua.army.mil. Follow the DA Form 2028 format or submit an electronic DA Form 2028.

Unless otherwise stated, masculine nouns and pronouns do not refer exclusively to men. Use of the terms "he" and "him" in this manual should be read as referring to both males and females unless otherwise expressly noted.

PART ONE

HUMINT Support, Planning, and Management

HUMINT collection activities include three general categories: screening, interrogation, and debriefing. In some cases these may be distinguished by legal distinctions between source categories such as between interrogation and debriefing. In others, the distinction is in the purpose of the questioning. Regardless of the type of activity, or goal of the collection effort, HUMINT collection operations must be characterized by effective support, planning, and management.

Chapter 1

Introduction

INTELLIGENCE BATTLEFIELD OPERATING SYSTEM

1-1. The Intelligence battlefield operating system (BOS) is one of seven operating systems—Intelligence, maneuver, fire support, air defense, mobility/countermobility/survivability, combat service support (CSS), and command and control—that enable commanders to build, employ, direct, and sustain combat power. The Intelligence BOS is a flexible force of Intelligence personnel, organizations, and equipment. Individually and collectively, these assets generate knowledge of and products portraying the enemy and the environmental features required by a command planning, preparing, executing, and assessing operations. Inherent within the Intelligence BOS is the capability to plan, direct, and synchronize intelligence, surveillance, and reconnaissance (ISR) operations; collect and process information; produce relevant intelligence; and disseminate intelligence and critical information in an understandable and presentable form to those who need it, when they need it. As one of the seven disciplines of the Intelligence BOS, HUMINT provides a capability to the supported commander in achieving information superiority on the battlefield.

INTELLIGENCE PROCESS

1-2. Intelligence operations consist of the functions that constitute the intelligence process: **plan, prepare, collect, process, produce**, and the common tasks of **analyze, disseminate,** and **assess** that occur throughout the intelligence process. Just as the activities of the operations process overlap and recur as circumstances demand, so do the functions of the intelligence process. Additionally, the analyze, disseminate, and assess tasks

of the intelligence process occur continuously throughout the intelligence process. (See Figure 1-1.)

- **Plan**. This step of the intelligence process consists of activities that include assessing the situation, envisioning a desired outcome (also known as setting the vision), identifying pertinent information and intelligence requirements, developing a strategy for ISR operations to satisfy those requirements, directing intelligence operations, and synchronizing the ISR effort. The commander's intent, planning guidance, and commander's critical information requirements (CCIRs) (priority information requirements [PIRs] and friendly force information requirements [FFIRs]) drive the planning of intelligence operations. Commanders must involve their supporting staff judge advocate (SJA) when planning intelligence operations (especially HUMINT operations). Planning, managing, and coordinating these operations are continuous activities necessary to obtain information and produce intelligence essential to decisionmaking.
- **Prepare**. This step includes those staff and leader activities that take place upon receiving the operations plan (OPLAN), operations order (OPORD), warning order (WARNO), or commander's intent to improve the unit's ability to execute tasks or missions and survive on the battlefield.
- **Collect.** Recent ISR doctrine necessitates that the entire staff, especially the G3/S3 and G2/S2, must change their reconnaissance and surveillance (R&S) mindset to conducting ISR. The staff must carefully focus ISR on the CCIR but also enable the quick re-tasking of units and assets as the situation changes. This doctrinal requirement ensures that the enemy situation, not just our OPLAN, "drives" ISR operations. Well-developed procedures and carefully planned flexibility to support emerging targets, changing requirements, and the need to support combat assessment are critical. The G3/S3 and G2/S2 play a critical role in this challenging task that is sometimes referred to as "fighting ISR" because it is so staff intensive during planning and execution (it is an operation within the operation). Elements of all units on the battlefield obtain information and data about enemy forces, activities, facilities, and resources as well as information concerning the environmental and geographical characteristics of a particular area.
- **Process.** This step converts relevant information into a form suitable for analysis, production, or immediate use by the commander. Processing also includes sorting through large amounts of collected information and intelligence (multidiscipline reports from the unit's ISR assets, lateral and higher echelon units and organizations, and non-MI elements in the battlespace). Processing identifies and exploits that information which is pertinent to the commander's intelligence requirements and facilitates situational understanding. Examples of processing include developing film, enhancing imagery, translating a document from a foreign language, converting electronic data into a standardized report that can be analyzed by a system operator, and

correlating dissimilar or jumbled information by assembling like elements before the information is forwarded for analysis.

- **Produce.** In this step, the G2/S2 integrates evaluated, analyzed, and interpreted information from single or multiple sources and disciplines into finished intelligence products. Like collection operations, the G2/S2 must ensure the unit's information processing and intelligence production are prioritized and synchronized to support answering the collection requirements.

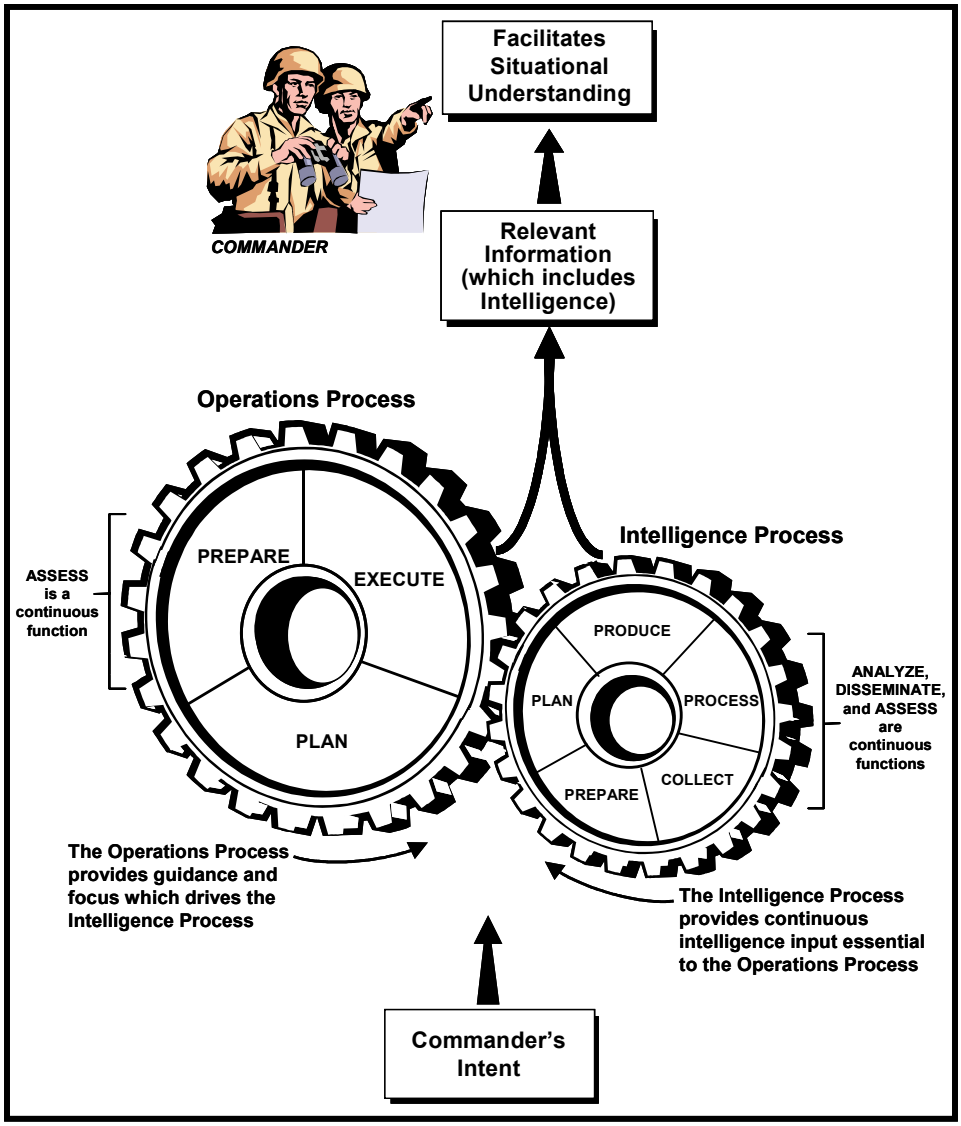


Figure 1-1. Intelligence Process.

1-3. For more information on the Intelligence process, see FM 2-0.

HUMAN INTELLIGENCE

1-4. HUMINT is the collection of information by a trained HUMINT collector (military occupational specialties [MOSs] 97E, 351Y [formerly 351C], 351M [formerly 351E], 35E, and 35F), from people and their associated documents and media sources to identify elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities. It uses human sources as a tool and a variety of collection methods, both passively and actively, to gather information to satisfy the commander's intelligence requirements and cross-cue other intelligence disciplines.

1-5. HUMINT tasks include but are not limited to—

- Conducting source operations.
- Liaising with host nation (HN) officials and allied counterparts.
- Eliciting information from select sources.
- Debriefing US and allied forces and civilian personnel including refugees, displaced persons (DPs), third-country nationals, and local inhabitants.
- Interrogating EPWs and other detainees.
- Initially exploiting documents, media, and materiel.

Note. In accordance with Army regulatory and policy guidance, a select set of intelligence personnel may be trained and certified to conduct certain HUMINT tasks outside of those which are standard for their primary MOS. Such selection and training will qualify these personnel to conduct only those specific additional tasks, and will not constitute qualifications as a HUMINT collector.

HUMINT SOURCE

1-6. A HUMINT source is a person from whom information can be obtained. The source may either possess first- or second-hand knowledge normally obtained through sight or hearing. Potential HUMINT sources include threat, neutral, and friendly military and civilian personnel. Categories of HUMINT sources include but are not limited to detainees, refugees, DPs, local inhabitants, friendly forces, and members of foreign governmental and non-governmental organizations (NGOs).

HUMINT COLLECTOR

1-7. For the purpose of this manual, a HUMINT collector is a person who is specifically trained and certified for, tasked with, and engages in the collection of information from individuals (HUMINT sources) for the purpose of answering intelligence information requirements. HUMINT collectors specifically include enlisted personnel in MOS 97E, Warrant Officers (WOs) in MOS 351M (351E) and MOS 351Y (351C), commissioned officers in MOS 35E and MOS 35F, select other specially trained MOSs, and their Federal civilian employee and civilian contractor counterparts. These specially trained and certified individuals are the **only** personnel authorized to conduct HUMINT collection operations, although CI agents also use HUMINT collection techniques in the conduct of CI operations. HUMINT

collection operations must be conducted in accordance with applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. Additional policies and regulations apply to management of contractors engaged in HUMINT collection. (See Bibliography for additional references on contractor management.) HUMINT collectors are not to be confused with CI agents, MOS 97B and WO MOS 351L (351B). CI agents are trained and certified for, tasked with, and carry out the mission of denying the enemy the ability to collect information on the activities and intentions of friendly forces. Although personnel in 97E and 97B MOSs may use similar methods to carry out their missions, commanders should not use them interchangeably. See Figure 1-2 for HUMINT and CI functions.

PHASES OF HUMINT COLLECTION

1-8. Every HUMINT questioning session, regardless of the methodology used or the type of operation, consists of five phases. The five phases of HUMINT collection are planning and preparation, approach, questioning, termination, and reporting. They are generally sequential; however, reporting may occur at any point within the process when critical information is obtained and the approach techniques used will be reinforced as required through the questioning and termination phases.

Planning and Preparation

1-9. During this phase, the HUMINT collector conducts the necessary research and operational planning in preparation for a specific collection effort with a specific source. Chapter 7 discusses this phase in detail.

Approach

1-10. During the approach phase, the HUMINT collector establishes the conditions of control and rapport to gain the cooperation of the source and to facilitate information collection. Chapter 8 discusses approach and termination strategies in detail.

Questioning

1-11. During the questioning phase, the HUMINT collector uses an interrogation, debriefing, or elicitation methodology to ask a source questions systematically on relevant topics, collect information in response to the intelligence tasking, and ascertain source veracity. Chapter 9 discusses questioning techniques in detail. (See Appendix B for a source and reliability matrix.)

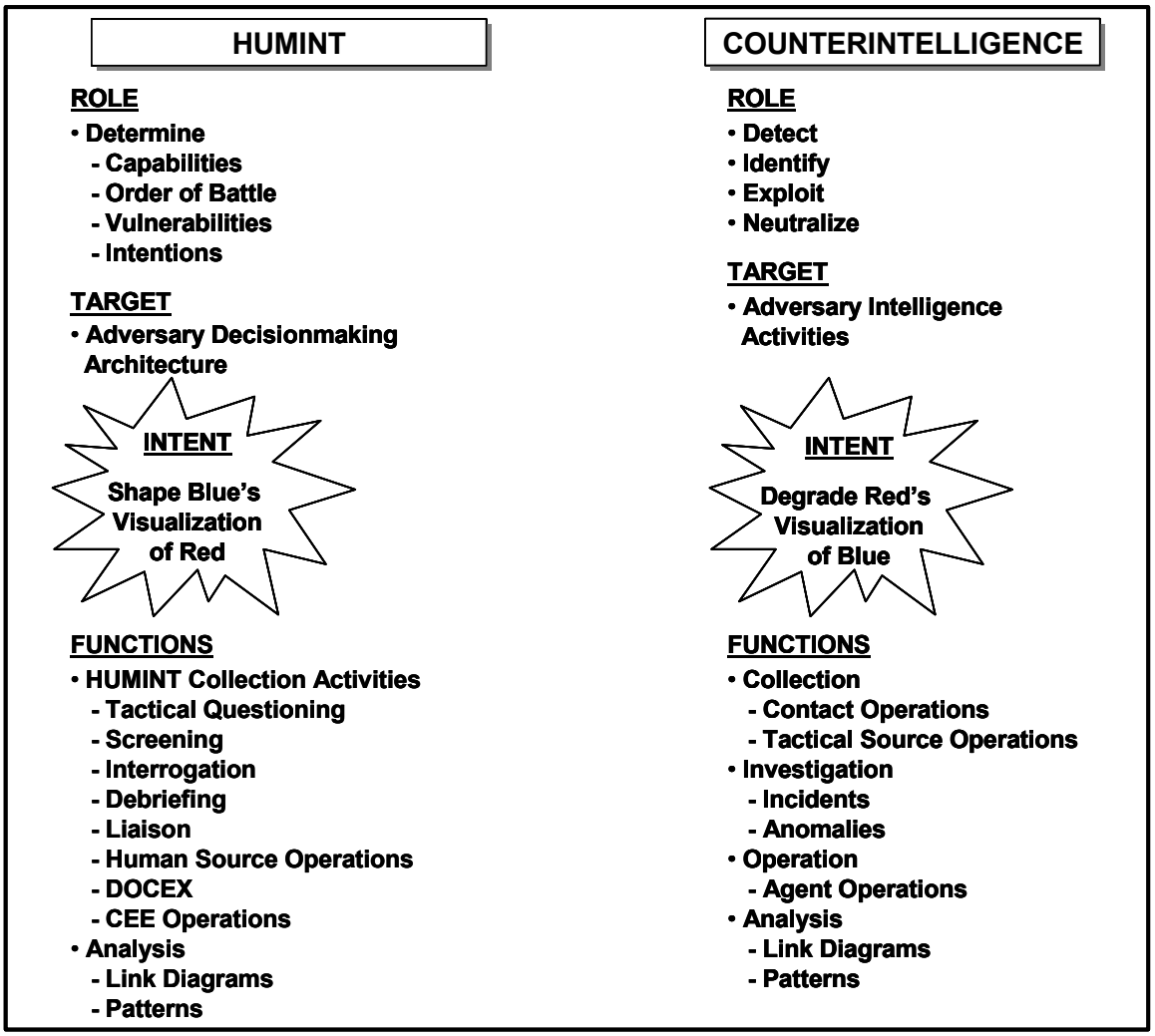


Figure 1-2. HUMINT and CI Functions.

Termination

1-12. During the termination phase, the HUMINT collector completes a questioning session and establishes the necessary conditions for future collection from the same source by himself or another HUMINT collector. (See Chapter 8.)

Reporting

1-13. During the reporting phase, the HUMINT collector writes, edits, and submits written, and possibly oral, reports on information collected in the course of a HUMINT collection effort. These reports will be reviewed, edited, and analyzed as they are forwarded through the appropriate channels. Chapter 10 discusses reporting in detail.

HUMINT COLLECTION AND RELATED ACTIVITIES

1-14. HUMINT collection activities include these categories: tactical questioning, screening, interrogation, debriefing, liaison, human source contact operations (SCOs), document exploitation (DOCEX), and captured enemy equipment (CEE) operations. DOCEX and CEE operations are activities supported by HUMINT collection but usually are only conducted by HUMINT collectors when the CEE or captured enemy document (CED) is associated with a source being questioned. In some cases, these determinations may depend on legal distinctions between collection methods such as interrogation and debriefing. In others, the distinction is in the purpose of the questioning. For example, screening is used to identify the knowledgeability and cooperation of a source, as opposed to the other activities that are used to collect information for intelligence purposes.

1-15. The activities may be conducted interactively. For example, a HUMINT collector may be screening a potential source. During the course of the screening, the HUMINT collector identifies that the individual has information that can answer requirements. He might at that point debrief or interrogate the source on that specific area. He will then return to screening the source to identify other potential areas of interest.

1-16. HUMINT collection activities vary depending on the source of the information. Once the type of activity has been determined, leaders use the process of plan, prepare, execute, and assess to conduct the activity. The following are the different types of HUMINT collection activities.

TACTICAL QUESTIONING

1-17. Tactical questioning is expedient initial questioning for information of immediate tactical value. Tactical questioning is generally performed by members of patrols, but can be done by any DOD personnel. (See ST 2-91.6.)

SCREENING

1-18. Screening is the process of identifying and assessing the areas of knowledge, cooperation, and possible approach techniques for an individual who has information of intelligence value. Indicators and discriminators used in screening can range from general appearance, possessions, and attitude to specific questions to assess areas of knowledge and degree of cooperation to establish if an individual matches a predetermined source profile. Screening is not in itself an intelligence collection technique but a timesaving measure that identifies those individuals most likely to have information of value.

1-19. Screening operations are conducted to identify the level of knowledge, level of cooperation, and the placement and access of a given source. Screening operations can also assist in the determination of which discipline or agency can best conduct the exploitation. Chapter 6 discusses screening in detail. Screening operations include but are not limited to—

- Mobile and static checkpoint screening, including screening of refugees and DPs.
- Locally employed personnel screening.

- Screening as part of a cordon and search operation.
- EPW and detainee screening.

INTERROGATION

1-20. Interrogation is the systematic effort to procure information to answer specific collection requirements by direct and indirect questioning techniques of a person who is in the custody of the forces conducting the questioning. Some examples of interrogation sources include EPWs and other detainees. Interrogation sources range from totally cooperative to highly antagonistic. Interrogations may be conducted at all echelons in all operational environments. Detainee interrogation operations conducted at a Military Police (MP) facility, coalition-operated facility, or other agency-operated collection facility are more robust and require greater planning, but have greater logistical support. Interrogations may only be conducted by personnel trained and certified in the interrogation methodology, including personnel in MOSs 97E, 351M (351E), or select others as may be approved by DOD policy. Interrogations are always to be conducted in accordance with the Law of War, regardless of the echelon or operational environment in which the HUMINT collector is operating.

DEBRIEFING

1-21. Debriefing is the process of questioning cooperating human sources to satisfy intelligence requirements, consistent with applicable law. The source usually is not in custody and usually is willing to cooperate. Debriefing may be conducted at all echelons and in all operational environments. The primary categories of sources for debriefing are refugees, émigrés, DPs, and local civilians; and friendly forces.

- **Refugees, Émigrés, DPs, and Local Civilians Debriefing Operations.** Refugee, émigré, and DP debriefing operations are the process of questioning cooperating refugees and émigrés to satisfy intelligence requirements. The refugee may or may not be in custody, and a refugee or émigré's willingness to cooperate need not be immediate or constant. Refugee debriefings are usually conducted at refugee collection points or checkpoints and may be conducted in coordination with civil affairs (CA) or MP operations. Local civilian debriefing operations are the process of questioning cooperating local civilians to satisfy intelligence requirements. As with refugees and émigrés, the local civilians being debriefed may or may not be in custody and the civilian's willingness to cooperate may not be immediate or constant. Debriefing operations must be conducted consistent with applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs.
- **Friendly Force Debriefing Operations.** Friendly force debriefing operations are the systematic debriefing of US forces to answer

collection requirements. These operations must be coordinated with US units. (See Chapter 6.)

LIAISON OPERATIONS

1-22. Liaison operations are programs to coordinate activities and exchange information with host country and allied military and civilian agencies and NGOs.

HUMAN SOURCE CONTACT OPERATIONS

1-23. Human SCO are operations directed toward the establishment of human sources who have agreed to meet and cooperate with HUMINT collectors for the purpose of providing information. Within the Army, SCO are conducted by trained personnel under the direction of military commanders. The entire range of HUMINT collection operations can be employed. SCO sources include one-time contacts, continuous contacts, and formal contacts from debriefings, liaison, and contact operations. SCO consist of collection activities that utilize human sources to identify attitude, intentions, composition, strength, dispositions, tactics, equipment, target development, personnel, and capabilities of those elements that pose a potential or actual threat to US and coalition forces. SCO are also employed to develop local source or informant networks that provide early warning of imminent danger to US and coalition forces and contribute to the Military Decision-Making Process (MDMP). See Chapter 5 for discussion of approval, coordination, and review for each type of activity.

DOCEX OPERATIONS

1-24. DOCEX operations are the systematic extraction of information from open, closed, published, and electronic source documents. These documents may include documents or data inside electronic communications equipment, including computers, telephones, Personal Digital Assistants (PDAs), and Global Positioning System (GPS) terminals. This operation is not solely a HUMINT function, but may be conducted by any intelligence personnel with appropriate language support.

1-25. Many CEDs are associated with EPWs and other human sources. Consequently, a HUMINT collector is often the first person to screen them. HUMINT collectors will screen the documents associated with human sources and will extract information of use to them in their immediate collection operation. Any information discovered during this initial screening that might cross-cue another collection effort will be forwarded to the appropriate unit.

1-26. A captured document is usually something that the enemy has written for his own use. For this reason, captured documents are usually truthful and accurate. There are cases in which falsified documents have been permitted to fall into enemy hands as a means of deception but these cases are not the norm. Normal policy of not relying on single-source information should help prevent deceptions of this type from being effective. Documents also do not forget or misinterpret information although it must be remembered that their authors may have. Usually, each document provides a portion of a

larger body of information. Each captured document, much like a single piece of a puzzle, contributes to the whole. In addition to tactical intelligence, technical data and political indicators that are important to strategic and national level agencies can sometimes be extracted from captured documents. Captured documents, while not affected by memory loss, are often time sensitive; therefore, they are to be quickly screened for possible exploitation.

CEE OPERATIONS

1-27. CEE includes all types of foreign and non-foreign materiel found on a detainee or on the battlefield that may have a military application or answer a collection requirement. The capturing unit must—

- Recognize certain CEE as having immediate intelligence value, and immediately forward such CEE to the unit's S2. Such items include—
 - All electronic communications equipment with a memory card, including computers, telephones, PDAs, and GPS terminals.
 - All video or photographic equipment.
- Recognize certain CEE as having technical intelligence (TECHINT) value. Such items include—
 - New weapons.
 - All communications equipment not immediately exploitable for HUMINT value.
 - Track vehicles.
 - Equipment manuals.
 - All CEE known or believed to be of TECHINT interest.
- Evacuate the equipment with the detainee.
- Confiscate, tag, and evacuate weapons and other equipment found on the detainee the same as CEDs. (See Appendix D.)
- Secure and report the capture of TECHINT items to the unit's S2 for disposition instructions.

TRAITS OF A HUMINT COLLECTOR

1-28. HUMINT collection is a science and an art. Although many HUMINT collection skills may be taught, the development of a skilled HUMINT collector requires experience in dealing with people in all conditions and under all circumstances. Although there are many intangibles in the definition of a "good" HUMINT collector, certain character traits are invaluable:

- **Alertness.** The HUMINT collector must be alert on several levels while conducting HUMINT collection. He must concentrate on the information being provided by the source and be constantly evaluating the information for both value and veracity based on collection requirements, current intelligence, and other information obtained from the source. Simultaneously, he must be alert not only to what the source says but also to how it is said and the accompanying body language to assess the source's truthfulness, degree of cooperation, and current mood. He needs to know when to give the source a break and

when to press the source harder. In addition, the HUMINT collector constantly must be alert to his environment to ensure his personal security and that of his source.

- **Patience and Tact.** The HUMINT collector must have patience and tact in creating and maintaining rapport between himself and the source, thereby enhancing the success of the questioning. Displaying impatience may—
 - Encourage a difficult source to think that if he remains unresponsive for a little longer, the HUMINT collector will stop questioning.
 - Cause the source to lose respect for the HUMINT collector, thereby reducing the HUMINT collector's effectiveness.
- **Credibility.** The HUMINT collector must provide a clear, accurate, and professional product and an accurate assessment of his capabilities. He must be able to clearly articulate complex situations and concepts. The HUMINT collector must also maintain credibility with his source. He must present himself in a believable and consistent manner, and follow through on any promises made as well as never to promise what cannot be delivered.
- **Objectivity and Self-control.** The HUMINT collector must also be totally objective in evaluating the information obtained. The HUMINT collector must maintain an objective and dispassionate attitude regardless of the emotional reactions he may actually experience or simulate during a questioning session. Without objectivity, he may unconsciously distort the information acquired. He may also be unable to vary his questioning and approach techniques effectively. He must have exceptional self-control to avoid displays of genuine anger, irritation, sympathy, or weariness that may cause him to lose the initiative during questioning but be able to fake any of these emotions as necessary. He must not become emotionally involved with the source.
- **Adaptability.** A HUMINT collector must adapt to the many and varied personalities which he will encounter. He must also adapt to all types of locations, operational tempos, and operational environments. He should try to imagine himself in the source's position. By being adaptable, he can smoothly shift his questioning and approach techniques according to the operational environment and the personality of the source.
- **Perseverance.** A tenacity of purpose can be the difference between a HUMINT collector who is merely good and one who is superior. A HUMINT collector who becomes easily discouraged by opposition, non-cooperation, or other difficulties will not aggressively pursue the objective to a successful conclusion or exploit leads to other valuable information.
- **Appearance and Demeanor.** The HUMINT collector's personal appearance may greatly influence the conduct of any HUMINT collection operation and attitude of the source toward the HUMINT collector. Usually an organized and professional appearance will favorably influence the source. If the HUMINT collector's manner

reflects fairness, strength, and efficiency, the source may prove more cooperative and more receptive to questioning.

- **Initiative.** Achieving and maintaining the initiative are essential to a successful questioning session just as the offensive is the key to success in combat operations. The HUMINT collector must grasp the initiative and maintain it throughout all questioning phases. This does not mean he has to dominate the source physically; rather, it means that the HUMINT collector knows his requirements and continues to direct the collection toward those requirements.

REQUIRED AREAS OF KNOWLEDGE

1-29. The HUMINT collector must be knowledgeable in a variety of areas in order to question sources effectively. The collector must prepare himself for operations in a particular theater or area of intelligence responsibility (AOIR) by conducting research. The G2 can be a valuable source of information for this preparatory research. The HUMINT collector should consult with order of battle (OB) technicians and analysts and collect information from open sources and from the Secret Internet Protocol Router Network (SIPRNET) to enhance his knowledge of the AOIR. Some of these areas of required knowledge are—

- **The area of operations (AO)** including the social, political, and economic institutions; geography; history; language; and culture of the target area. Collectors must be aware of all ethnic, social, religious, political, criminal, tribal, and economic groups and the interrelationships between these groups.
- **All current and potential threat forces** within the AOIR and their organization, equipment, motivation, capabilities, limitations, and normal operational methodology.
- **Applicable law and policy that might affect HUMINT collection activities. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs.** HUMINT collectors are subject to applicable law, which includes US law, the law of war (including the Geneva Conventions as applicable), and relevant international law. Additionally, local agreements with HNs or allies and the applicable execute orders and rules of engagement (ROE) may further restrict HUMINT collection activities. However, these documents cannot permit interrogation actions that would be illegal under applicable US or international law.
- **The collection requirements,** including all specific information requirements (SIRs) and indicators that will lead to the answering of the intelligence requirements.

- **Cultural awareness** in the various AOs will have different social and regional considerations that affect communications and can affect the conduct of operations. These may include social taboos, desired behaviors, customs, and courtesies. The staff must include this information in pre-deployment training at all levels to ensure that personnel are properly equipped to interact with the local populace.

1-30. There are other areas of knowledge that help to develop more effective questioning:

- **Proficiency in the target language**. The HUMINT collector can normally use an interpreter (see Chapter 11) and machine translation as they are developed to conduct questioning. Language proficiency is a benefit to the HUMINT collector in a number of ways: He can save time in questioning, be more aware of nuances in the language that might verify or deny truthfulness, and better control and evaluate interpreters.
- **Understanding basic human behavior**. A HUMINT collector can best adapt himself to the source's personality and control of the source's reactions when he understands basic behavioral factors, traits, attitudes, drives, motivations, and inhibitions. He must not only understand basic behavioral principles but also know how these principles are manifested in the area and culture in which he is operating.
- **Neurolinguistics**. Neurolinguistics is a behavioral communication model and a set of procedures that improve communication skills. The HUMINT collector should read and react to nonverbal communications. He must be aware of the specific neurolinguistic clues of the cultural framework in which he is operating.

CAPABILITIES AND LIMITATIONS

CAPABILITIES

1-31. HUMINT collection capabilities include the ability to—

- Collect information and cross-cue from an almost endless variety of potential sources including friendly forces, civilians, detainees, and source-related documents.
- Focus on the collection of detailed information not available by other means. This includes information on threat intentions and local civilian and threat force attitudes and morale. It also includes building interiors and facilities that cannot be collected on by other means due to restrictive terrain.
- Corroborate or refute information collected from other R&S assets.
- Operate with minimal equipment and deploy in all operational environments in support of offensive, defensive, stability and reconstruction operations, or civil support operations. Based on solid planning and preparation, HUMINT collection can provide timely information if deployed forward in support of maneuver elements.

LIMITATIONS

1-32. HUMINT collection limitations include—

- Interpersonal abilities. HUMINT is dependent on the subjective interpersonal capabilities of the individual rather than on the abilities to operate collection equipment. HUMINT collection capability is based on experience within a specific AO that can only be developed over time.
- Identification of knowledgeable sources. There is often a multitude of potential HUMINT sources. Information in response to specific requirements can only be collected if sources are available and identified that have that information.
- Limited numbers. There are never enough HUMINT collectors to meet all requirements. Limited assets must be prioritized in support of units and operations based on their criticality.
- Time limitations. HUMINT collection, particularly source operations, takes time to develop. Collection requirements must be developed with sufficient lead-time for collection.
- Language limitations. Although HUMINT collectors can normally use an interpreter, a lack of language proficiency by the collector can significantly slow collection efforts. Such language proficiency takes time to develop.
- Misunderstanding of the HUMINT mission. HUMINT collectors are frequently used incorrectly and assigned missions that belong to CA, MP, interpreter or translators, CI, or other operational specialties.
- Commanders' risk management. Maneuver commanders, in weighing the risks associated with employing HUMINT collection teams (HCTs), should seriously consider the potential loss of a wealth of information such as enemy activities, locations of high-value personnel, and threats to the force that they will incur if they restrict HCT collection activities. J/G2Xs, operational management teams (OMTs), and HCT leaders must educate maneuver commanders on the benefits of providing security for HCTs and employing them in accordance with their capabilities.
- Legal obligations. Applicable law and policy govern HUMINT collection operations. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. HUMINT operations may be further restricted by Status of Forces Agreements (SOFAs) and other agreements, execute orders and ROE, local laws, and an operational umbrella concept. Such documents, however, cannot permit interrogation actions that are illegal under applicable law.
- Connectivity and bandwidth requirements. With the exception of the size, activity, location, unit, time, equipment (SALUTE) report, most HUMINT reporting requires considerable bandwidth. Deployed

HUMINT teams must be able to travel to, and report from, all areas of the battlefield. Digital communication equipment must be able to provide reliable connectivity with teams' reporting channels and sufficient bandwidth for transmission of reports, including digital imagery.

- Timely reporting and immediate access to sources. Except in tactical situations when HUMINT collectors are in immediate support of maneuver units, HUMINT collection and reporting takes time. In stability and reconstruction operations, sources need to be assessed and developed. Once they are developed, they need to be contacted which often takes time and coordination. In offensive and defensive operations, HUMINT collection at detainee holding areas sometimes may still be timely enough to meet tactical and operational requirements. See paragraphs 3-2 and 3-7 for more information on offensive and defensive operations.

This page intentionally left blank.

Chapter 2

Human Intelligence Structure

ORGANIZATION AND STRUCTURE

2-1. The success of the HUMINT collection effort depends on a complex interrelationship between command and control (C2) elements, requirements, technical control and support, and collection assets. Each echelon of command has its supporting HUMINT elements although no MI organization in the Army is robust enough to conduct sustained HUMINT operations under all operational environments using only its organic HUMINT assets. HUMINT units have specific support requirements to the commander. HUMINT units must be flexible, versatile, and prepared to conduct HUMINT collection and analysis operations in support of any echelon of command. A coherent C2 structure within these HUMINT organizations is necessary in order to ensure successful, disciplined, and legal HUMINT operations. This structure must include experienced commissioned officers, warrant officers, and senior NCOs conscientiously discharging their responsibilities and providing HUMINT collectors with guidance from higher headquarters.

2-2. Regardless of the echelon, there are four basic elements that work together to provide the deployed commander with well-focused, thoroughly planned HUMINT support. The four elements are staff support, analysis, C2, and collection. Each piece of the infrastructure builds on the next and is based on the size, complexity, and type of operation as shown in Figure 2-1.

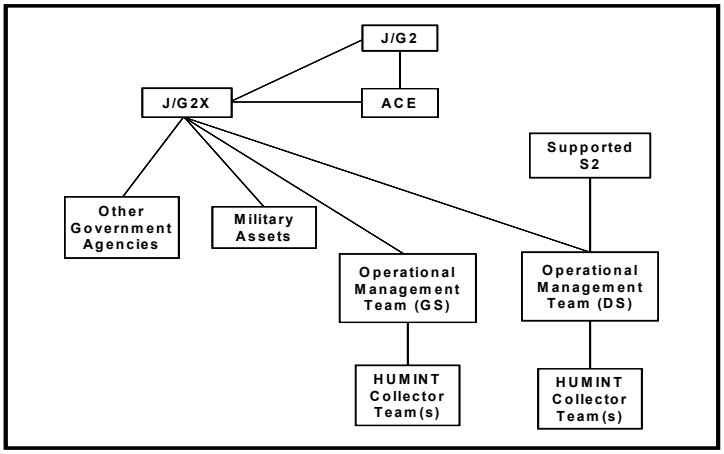


Figure 2-1. Tactical HUMINT Organization.

HUMINT CONTROL ORGANIZATIONS

2-3. HUMINT control organizations are the means by which a commander exercises command of a unit's operations. HUMINT control organizations are vital to the effective use of HUMINT collection assets. HUMINT control organizations consist of the C/J/G/S2X and the HUMINT operations cell (HOC) at the brigade and above level and the OMTs at the battalion and below level.

C/J/G/S2X

2-4. The C/J/G/S2X is a staff element subordinate to the C/J/G/S2, is the primary advisor on HUMINT and CI, and is the focal point for all HUMINT and CI activities within a joint task force (JTF) (J2X), an Army component task force (G2X) or a brigade combat team (BCT) (S2X). The 2X can be organic to the unit staff or can be attached or under operational control (OPCON) to the staff from another organization such as the theater MI brigade. The C/J/G/S2X is part of a coherent architecture that includes organic HUMINT assets and HUMINT resources from national, theater, and non-DOD HUMINT organizations.

2-5. The C/J2X is responsible for controlling Joint Force HUMINT assets, coordinating all HUMINT and CI collection activities, and keeping the joint force C/J/2 informed on all HUMINT and CI activities conducted in the joint force area of responsibility (AOR). The C/J2X is also part of the review and recommendation process concerned with the retention or release of detainees. HUMINT reports maintained at the C/J2X are considered during the review for release process. The C/J2X consists of the 2X Officer, a HOC, a Counterintelligence Coordination Authority (CICA), a HUMINT Analysis Cell (HAC), and a CI Analysis Cell (CIAC). At all echelons, the 2X should also include an Operational Support Cell (OSC) staffed to operate 24 hours a day. The authority and operational responsibilities of a C/J2X in combined or joint contingency operations (CONOP) takes precedence over service-specific CI and HUMINT technical control agencies. Specifically, the C/J/G/S2X—

- Accomplishes technical control and support, and deconfliction of all HUMINT and CI assets through the Army component G2X, the HUMINT and CI operations sections, or the OMTs.
- Participates in planning for deployment of HUMINT and CI assets in support of operations.
- Coordinates, through the HOC and the CICA, all HUMINT and CI activities to support intelligence collection and the intelligence aspects of force protection for the deployed commander.
- Coordinates and deconflicts all HUMINT and CI operations within the operational area.
- Coordinates with the senior US national intelligence representative for specific operational approval when required by standing agreements.
- Is the release authority for HUMINT reporting at his echelon and only releases reports to the all-source system after ensuring all technical control measures for reporting have been met.

- Coordinates with other HUMINT collection agencies not under the control of the command, such as Defense Intelligence Agency (DIA), Central Intelligence Agency (CIA), and Federal Bureau of Investigation (FBI).
- Does not exercise OPCON over HUMINT and CI assets assigned, attached, or reinforcing the unit; however, he is the staff support responsible for creating a cohesive HUMINT and CI effort.
- Coordinates with non-DOD agencies conducting HUMINT collection operations in the joint area of operations (JAO) to ensure deconfliction of sources, informants, or contacts and the HUMINT reporting that is generated by these collection operations.

2-6. The J2X will maintain technical control (see para 4-10) of all CI investigative actions within its AOIR; however, all investigative matters will be in accordance with DOD policies, joint or Military Department doctrine, applicable US law and policy, SOFAs, or other International Standardization Agreements (ISAs). The J2X will advise the responsible Theater CICA (TCICA) of any Army CI element conducting investigative activities that fall under the purview of AR 381-20.

OPERATIONS SUPPORT CELL (OSC)

2-7. The OSC in the C/J/G/S2X staff will maintain the consolidated source registry for all HUMINT and CI activities in the unit's designated AOIR. The OSC will provide management of intelligence property book operations, source incentive programs, and intelligence contingency funds (ICFs) for subordinate HUMINT and CI elements. The OSC responsibilities also include requests for information (RFIs) and/or source-directed requirements (SDRs) management and the release of intelligence information reports (IIRs).

COUNTERINTELLIGENCE COORDINATION AUTHORITY

2-8. The CICA is assigned under the J/G2X and coordinates all CI activities within its designated AOIR. (See FM 34-60 for a detailed explanation of the CI mission.) The CICA—

- Provides technical support to all CI assets and coordinates and deconflicts CI activities in the deployed AOIR.
- Coordinates and supervises CI investigations and collection activities conducted by all services and components in the AOIR.
- Establishes and maintains the theater CI source database.
- Coordinates with the HOC for CI support to detention, interrogation, refugee, and other facilities.
- Manages requirements and taskings for CI collectors in the AO in coordination with the HOC.
- Expedites preparation of CI reports and their distribution to consumers at all levels.
- Coordinates CI activities with senior CI officers from all CI organizations on the battlefield.

- Performs liaison with HN and US national level CI organizations.
- Informs the appropriate TCICA when Army CI elements are conducting CI investigative activities within the purview of AR 381-20.

HUMINT OPERATIONS CELL

2-9. The HOC is assigned under the J/G2X to track all HUMINT activities in the AOIR. The J/G2X uses this information to advise the senior intelligence officer (SIO) on all HUMINT activities conducted within the AOIR. The HOC—

- Provides technical support to all HUMINT collection operations and deconflicts HUMINT collection operations in the designated AOIR.
- Establishes and maintains a consolidated HUMINT source database in coordination with the CICA.
- Coordinates with collection managers and the HAC to identify collection requirements and to ensure requirements are met.
- Coordinates the activities of HUMINT collectors assigned or attached to interrogation, debriefing, refugee, DOCEX, and other facilities.
- Manages requirements and taskings for HUMINT collectors in the AOIR, in coordination with the CICA.
- Expedites preparation of intelligence reports and their distribution to consumers at all levels.
- Performs liaison with HN and US national HUMINT organizations.

OPERATIONAL MANAGEMENT TEAM

2-10. A HUMINT OMT consists of senior individuals in MOS 351M (351E) and MOS 97E. Each OMT can control 2 to 4 HCTs depending upon assigned mission and operational tempo (OPTEMPO). The OMT performs a necessary function when two or more HCTs deploy by assisting the HUMINT element commander in tasking and providing technical support to assigned or attached HCTs. The OMT is optimally collocated with the command post (CP) of the supported unit. However, it must be located where it can provide oversight of team operations and best support the dissemination of tasking, reports, and technical data between the unit and the deployed collection assets. When a higher echelon augments subordinate elements with collection teams, it should include proportional OMT augmentation. When a single collection team is attached in direct support (DS) of a subordinate element, the senior team member exerts mission and technical control over the team. The OMT—

- Provides operational and technical control and guidance to deployed HCTs.
- Normally consists of a WO and noncommissioned officers (NCOs) whose experience and knowledge provide the necessary guidance for effective team collection operations.
- Manages the use of ICFs and incentives for the HCTs.
- Provides the collection focus for HCTs.

- Provides quality control and dissemination of reports for subordinate HCTs.
- Directs the activities of subordinate HCTs and controls their operations.
- Conducts limited single-discipline HUMINT analysis and mission analysis for the supported commander.
- Acts as a conduit between subordinate HCTs, the HOC, and the C/J/G/S2X.
- Reports the HCT mission and equipment status to the HOC and the command element.

HUMINT COLLECTION TEAM

2-11. HCTs are the elements that collect information from human sources. The HUMINT collectors deploy in teams of approximately four personnel in MOS 97E (HUMINT Collector) and MOS 351M (351E) (HUMINT Technician).

2-12. The HCT may be augmented based on factors of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC). Interpreters from the RC or civilian contractors with appropriate security clearances are added when necessary. TECHINT personnel or other specific subject-matter experts (SMEs) may augment the team to meet technical collection requirements. Another example would be pairing HUMINT collectors with dedicated analysts to provide sharper focus to the interrogation effort. In fixed detention facilities, these HUMINT collector or analyst relationships may become more enduring. Commanders are not encouraged to mix HUMINT collectors and CI agents on a single team. Doing so seriously undermines the ability to conduct both the HUMINT collection and CI missions simultaneously. However, commanders may find times when METT-TC factors make it reasonable to augment a CI team with HUMINT support for a mission, or vice versa.

COMMAND DEBRIEFING TEAM

2-13. A command debriefing team is normally not a table of organization and equipment (TOE) organization but may be task organized to meet mission requirements. This task-organized team is normally OPCON to the HOC. Although more prevalent during stability and reconstruction operations, senior personnel will often acquire information of intelligence interest during the normal course of their duties. The HUMINT collection assets, particularly at division echelon or higher, will normally task organize a team of more senior, experienced individuals to debrief these senior unit personnel. In offensive and defensive operations, this same team is prepared to interrogate high-value detainees (including EPWs) or debrief senior civilians. The command debriefing team should not be confused with the G2/S2 debriefing program, which also is critical and is an important conduit of information.

DOCUMENT EXPLOITATION TEAM

2-14. DOCEX teams are normally found at theater and national level organizations. Lower echelon HCTs may also be designated to perform the DOCEX mission based upon mission parameters and linguist availability. However, if organic assets are used, there will be a mission tradeoff. Dependent on the priority of exploitation and volume of documents, HCTs assigned the DOCEX mission may be augmented by military, civilian, or contractor personnel to accomplish their assigned mission. During operations, the DOCEX team will normally screen documents, extract information, and expedite the evacuation of documents to the Joint or Theater Document Exploitation Facility.

HUMINT ANALYSIS AND PRODUCTION ORGANIZATIONS

2-15. HUMINT analysis and production organizations analyze information collected from HUMINT sources, support the requirements management (RM) system, and produce single-discipline intelligence products. HUMINT analysis and production are conducted at all echelons, separate brigades, and higher. (See Chapter 12 for a description of the HUMINT analysis system and methodologies.)

HUMINT ANALYSIS CELL

2-16. The HAC is part of the J/G2X; however, it may be collocated with an analysis and control element (ACE) or Joint Intelligence Support Element (JISE) single-source enclave depending on facilities and operational environment considerations. The HAC works closely with the all-source intelligence elements and the CIAC to ensure that HUMINT reporting is incorporated into the all-source analysis and common operational picture (COP). The HAC is the "fusion point" for all HUMINT reporting and operational analysis in the JISE and ACE. It determines gaps in reporting and coordinates with the RM to cross-cue other intelligence sensor systems. The HAC—

- Produces and disseminates HUMINT products and provides input to intelligence summaries (INTSUMs).
- Uses analytical tools found at the ACE or JISE to develop long-term analyses and provides reporting feedback that supports the HOC, OMTs, and HCTs.
- Provides analytical expertise to the C/J/G/S2X, HOC, and OMTs.
- Produces country and regional studies tailored to HUMINT collection.
- Compiles target folders to assist C/J/G/S2X assets in focusing collection efforts.
- Analyzes and reports on trends and patterns found in HUMINT reporting.
- Analyzes source reliability and credibility as reflected in reporting and communicates that analysis to the collector.
- Develops and maintains databases specific to HUMINT collection activities.
- Produces HUMINT requirements.

- Answers HUMINT-related RFIs.
- Identifies collection gaps and provides context for better collection at their echelon.

JOINT INTERROGATION AND DEBRIEFING CENTER ANALYSIS SECTION

2-17. This section ensures that all members of the Joint Interrogation and Debriefing Center (JIDC) (see para 5-102) are aware of the current situation through the distribution of INTSUMs and products from external agencies. The Analysis Section also supports the JIDC by—

- Providing situation update briefings to all facility personnel every 12 hours.
- Preparing research and background packets and briefings for interrogations and debriefings.
- Developing indicators for each intelligence requirement to support screening operations.
- Conducting single-discipline HUMINT analysis based on collected information to support further collection efforts.
- Correlating reports produced by the JIDC to facilitate analysis at higher levels.
- Answering RFIs from interrogators and formulating RFIs that cannot be answered by the analytical section on behalf of the interrogators.
- Reviewing IIRs and extracting information into analysis tools tailored to support the interrogation process.
- Pursuing products and resources to support the interrogation effort.

HUMINT ANALYSIS TEAM

2-18. The HUMINT analysis team (HAT) is subordinate to the G2 ACE. The HAT supports the G2 in the development of IPB products and in developing and tailoring SIRs to match HUMINT collection capabilities.

This page intentionally left blank.

Chapter 3

HUMINT in Support of Army Operations

3-1. Army doctrine for full spectrum operations recognizes four types of military operations: offensive, defensive, stability and reconstruction, and civil support. Missions in any environment require the Army to conduct or be prepared to conduct any combination of these operations. HUMINT assets will be called on to provide information in support of all four operations. Simultaneous operations, for example elements of a force conducting offensive operations while other elements are engaged in stability and reconstruction operations, will cause a similar division of the limited HUMINT assets based on METT-TC.

OFFENSIVE OPERATIONS

3-2. Offensive operations aim at destroying or defeating the enemy. Rapid maneuver, constantly changing situations, and a vital need for intelligence support at the point of contact influence HUMINT missions during offensive operations. The guiding principle to the use of HUMINT in support of offensive operations is to minimize the time between when friendly forces encounter potential sources (detainees, refugees, and local civilians) and when a HUMINT collector screens them.

3-3. During offensive operations, at echelons corps and below, HCTs normally operate in the engaged maneuver brigades' AOs and are further deployed in support of maneuver battalions based on advice from the OMTs. These collection assets may be in general support (GS) of the parent brigade or in DS of the maneuver battalions, reconnaissance squadrons, and other forward-deployed maneuver assets. The HCTs and their supporting control structure are deployed in accordance with METT-TC based on three principles:

- The relative importance of that subordinate element's operations to the overall parent unit's scheme of maneuver and the overall ISR plan.
- The potential for that subordinate element to capture detainees, media and materiel, or to encounter civilians on the battlefield.
- The criticality of information that could be obtained from those sources to the success of the parent unit's overall OPLANs.

3-4. HUMINT missions in support of offensive operations include screening and interrogating EPWs and other detainees, questioning and debriefing civilians in the supported unit's AO, and conducting DOCEX, limited to extracting information of immediate tactical value. EAC assets normally support offensive operations through theater interrogation and debriefing facility operations and mobile interrogation teams. These facilities are better equipped to conduct in-depth interrogations and DOCEX, so it is imperative

that EPWs and other detainees who will be evacuated to theater facilities be transported there as soon as possible.

HUMINT IN SUPPORT OF FORCED ENTRY OPERATIONS

3-5. Forced entry operations (FEOs) are offensive operations conducted to establish an initial military presence in a target area in the face of expected enemy opposition. HUMINT collection assets may be able to provide vital information to tactical commanders in the critical early stages of the entry operation. Key considerations for HUMINT support to FEOs include:

- HUMINT collectors attached or under OPCON of the initial force package to provide HUMINT collection support for the entry force. Collection teams will normally operate in support of battalion-sized or smaller elements. HUMINT collection assets should be integrated early and should participate in all aspects of planning and training, including rehearsals, to smoothly integrate and execute operations.
- HUMINT assets supporting the entry force must include proportional OMT elements. For example, if 2 to 4 teams are attached to a maneuver brigade, an OMT also needs to be attached. Even if the teams are further attached to maneuver battalions, there must be an OMT at the brigade level to coordinate and control HUMINT collection activities.
- HCTs and OMTs must be as mobile and as survivable as the entry forces. Team leaders should ensure that the supported unit will be able to provide maintenance support to the team vehicles, as appropriate, in accordance with the support relationship.
- Attached or OPCON HUMINT teams must have robust communications connectivity with the supported unit and must have reach connectivity through their OMT.
- HCTs must contain organic or attached language capability in order to conduct HUMINT collection effectively during FEO. It is unlikely that the teams can be augmented with attached civilian interpreters during this type of operation.

HUMINT IN SUPPORT OF EARLY ENTRY OPERATIONS

3-6. Early entry operations differ from FEOs in that early entry operations do not anticipate large-scale armed opposition. Early entry operations establish or enhance US presence, stabilize the situation, and shape the environment for follow-on forces. HUMINT collection provides critical support to defining the operational environment and assessing the threat to US forces. The considerations listed above for FEOs apply equally to early entry operations.

DEFENSIVE OPERATIONS

3-7. Defensive operations defeat an enemy attack, buy time, economize forces, hold the enemy in one area while attacking in another, or develop conditions favorable for offensive operations. Forces conducting defensive

operations must be able to identify rapidly the enemy's main effort and rapidly assess the operational conditions to determine the timing of counter-offensive or other operations. HUMINT support to defensive operations centers on the ability to provide the forward-deployed maneuver commander with information and intelligence of immediate tactical value. HUMINT assets should be placed in the AO of the forward elements to minimize the time between when friendly forces encounter potential sources (detainees, refugees, local civilians) and when a HUMINT collector screens them. HUMINT collectors are placed where the potential for HUMINT collection and the criticality of the information are greatest.

3-8. In defensive operations, it may be necessary to divide the HUMINT assets equally among the subordinate elements to provide area coverage until the primary enemy threat is identified. The HUMINT C2 elements (team leader, OMTs, and unit C2) must be prepared to task organize rapidly and shift resources as the situation dictates, based on the changing situation and higher headquarters FRAGO. HUMINT missions in defensive operations normally include interrogation of detainees, refugee debriefings, and assisting in friendly force patrol debriefings.

STABILITY AND RECONSTRUCTION OPERATIONS

3-9. Stability and reconstruction operations sustain and exploit security and control over areas, populations, and resources. They employ military and civilian capabilities to help establish order that advances US interests and values. The immediate goal often is to provide the local populace with security, restore essential services, and meet humanitarian needs. The long-term goal is to help develop indigenous capacity for securing essential services, a viable market economy, rule of law, democratic institutions, and robust civil society. Stability and reconstruction operations involve both coercive and cooperative actions. They may occur before, during, and after offensive and defensive operations; however, they also occur separately, usually at the lower end of the range of military operations. The primary focus of the HCTs during stability and reconstruction operations is to answer the commander's information requirements (IRs) and provide support to force protection. In stability and reconstruction operations, the HUMINT collectors must be able to maintain daily contact with the local population. The nature of the threat in stability operations can range from conventional forces to terrorists and organized crime and civil disturbances. Consequently, intelligence requirements can vary greatly. Examples of HUMINT collection requirements include TECHINT to support arms control; extensive political information and demographic data; order of battle (OB) regarding several different former warring factions during peace operations; or extremely detailed target data. HUMINT collectors also help to ascertain the feelings, attitudes, and activities of the local populace. Stability and reconstruction operations may be conducted in coordination with other US departments and agencies, and in conjunction with other countries and international organizations.

3-10. Centralized management and databasing are key to successful HUMINT operations. The HUMINT assets may operate in GS to the parent unit or operate in the AO of subordinate elements of the parent unit. For

example, in a division AO, the HCTs would normally operate in DS to the division but each team would normally have an AOIR that corresponds to the AO of the division's brigades or battalion task forces. There is close coordination between the HUMINT staff officer (C/J/G/S2X) and the OMTs to synchronize HUMINT operations properly, to develop the overall threat awareness, and to deconflict sources. The HCTs screen and debrief contacts to increase the security posture of US forces, to provide information in response to command collection requirements, and to provide early warning of threats to US forces. They may also interrogate detainees if permitted to do so by the mission-specific orders and in accordance with applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs.

3-11. Many stability and reconstruction operations are initiated with the establishment of a lodgment or base area. There is a subsequent expansion of operations to encompass the entire AO. The general concept of an HCT's operation is that of a two-phased effort. In the initial phase, the HCT establishes concentric rings of operations around the US forces starting from the supported unit's base of operations and working outward. Each ring is based on the threat environment and the commander's need to develop his knowledge of the tactical situation. The second, or continuation phase, begins once the initial information collection ring is established. The initial ring is not abandoned but rather is added to as the HCT shifts its focus to expand and establish the second and successive rings. The amount of time spent establishing each ring is situationally dependent.

INITIAL PHASE

3-12. The initial phase of stability and reconstruction operations is used to lay the foundation for future team operations. In general, the priority of effort is focused inward on security. The HCT conducts initial and follow-up screenings of locally employed personnel, to establish base data for subsequent source operations. The supported unit S2, with the assistance of the HUMINT team leader, establishes procedures to debrief reconnaissance and surveillance assets operating in the supported unit AO, as well as regular combat patrols or logistics convoys. The HCT lays the groundwork for future collection efforts by establishing liaison with local authorities, as well as developing plans and profiles for HUMINT collection. While establishing the initial and subsequent rings, the HCT actively seeks to collect PIR information, whether it pertains to the current ring or any other geographic location.

CONTINUATION PHASE

3-13. Following the initial phase, the HCT's focus shifts outward. While the HCT continues performing HUMINT collection and analysis functions within the base camp, it also expands its collection effort to outside the base camp to answer the supported unit's requirements. During the continuation phase, the HCT conducts contact operations with local personnel who may be able to

provide information of interest to the local commander or to satisfy the requirements of the tasking or request. The HCT also conducts liaison with local authorities, coalition forces (if present), NGOs, and others whose knowledge or activities may affect the success of the US mission. Any time the HCT is outside the base camp, it must be careful to observe the local population and report what it sees. The activities and attitudes of the general population will often have an effect on the commander's decisions on how to conduct US missions in the area.

LEVELS OF EMPLOYMENT

3-14. HCTs may be employed with varying degrees of contact with the local population. As the degree of contact with the population increases, the quantity and diversity of HUMINT collection increases. In many instances, however, there is a risk to the HCT inherent with increased exposure to the local population. The ability of the HCT members to fit in with the local populace can become very important to their safety. Consequently, the commander should consider exceptions to the ROE, as well as relaxed grooming and uniform standards, to help HCT members blend in and provide additional security. Commanders must consider the culture in which the HCT members will be operating. In some cultures, bearded men are more highly respected than clean-shaven men. Relaxing grooming standards for HCTs in these situations will support the team's ability to collect information. The decision regarding what level to employ an HCT is METT-TC dependent. The risk to the collection assets must be balanced with the need to collect information and to protect the force as a whole. The deployment and use of HUMINT collection assets may be limited by legal restrictions, mission-specific orders, directions from higher headquarters, and the overall threat level. The four basic levels of employment for the HCT are discussed below. Figure 3-1 shows these levels as well as their collection potential versus team security.

Base Camp

- Restricting the HCT to operations within the base camp minimizes the risk to the team. This action, however, minimizes the collection potential and maximizes the risk to the force as a whole. While restricted to a base camp, the HCT can maintain an extremely limited level of information collection by—
 - Interviewing walk-in sources and locally employed personnel.
 - Debriefing combat and ISR patrols.
 - Conducting limited local open-source information collection.
- This mode of deployment should be used only when dictated by operational restrictions. These would be at the initial stages of stability and reconstruction operations when the operational environment is being assessed, or as a temporary expedient when the force protection level exceeds the ability to provide reasonable protection for the collectors. A supported unit commander is often tempted to keep the HCT "inside the wire" when the force protection level or threat

condition (THREATCON) level increases. The supported unit and parent commanders must compare the gains of the HCT collection effort with the risks posed. This is necessary especially during high THREATCON levels when the supported unit commander needs as complete a picture as possible of the threat arrayed against US or multinational forces.

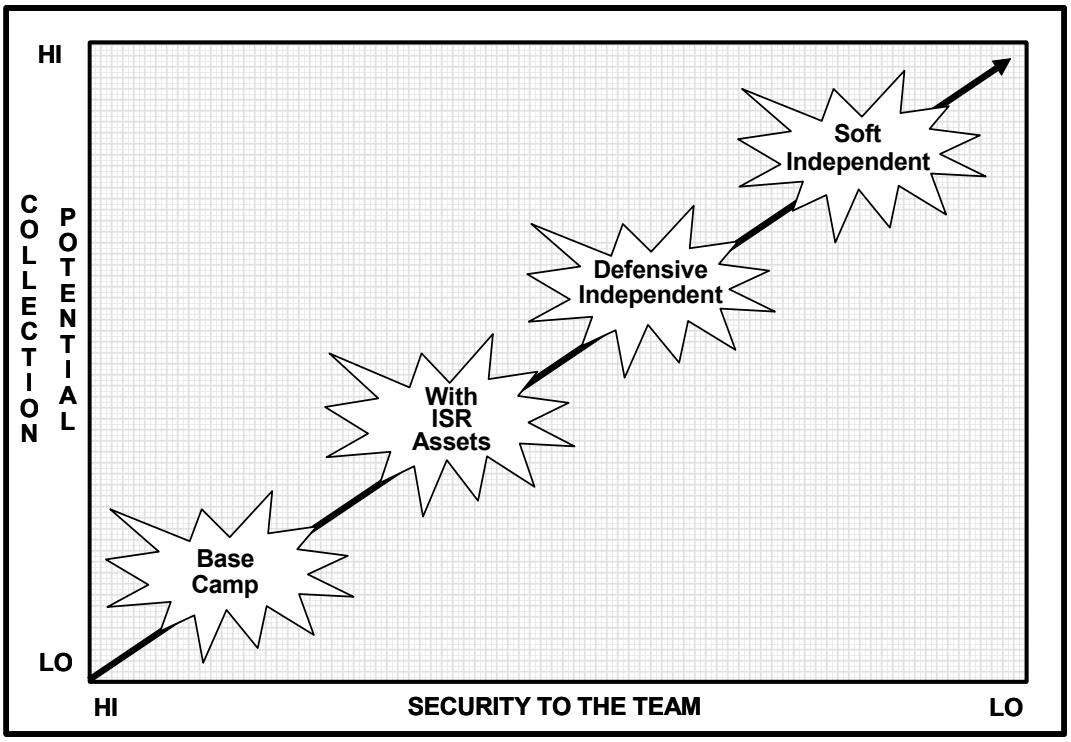


Figure 3-1. Team Level of Employment.

Integrated with Other Operations

- Under some circumstances, when it is not expedient to deploy the HCT independently due to threat levels or other restrictions, it can be integrated into other ongoing operations. The HCT may be employed as part of a combat patrol, ISR patrol, or in support of an MP patrol or stationed at a checkpoint or roadblock. It can also be used to support CA, psychological operations (PSYOP), engineer, or other operations. This method reduces the risk to the team while greatly increasing its collection potential over the confined-to-base-camp method. It has the advantage of placing the team in contact with the local population and allowing it to spot, assess, and interact with potential sources of information.
- The integration into other operations can also facilitate the elicitation of information. However, this deployment method restricts collection by subordinating the team's efforts to the requirements, locations, and timetables of the unit or operation into which it is integrated. Integration can be done at the team or individual collector level. HUMINT collectors should be used only in situations with an

intelligence collection potential. It is a waste of a valuable asset to use them in a function that could be performed by a civilian translator.

As an Independent Patrol

- Defensive. One of the key elements of the HCT success is the opportunity to spot, assess, and develop relationships with potential sources of information. Operating as independent patrols, without being tied to ISR or combat assets, enables the HCTs maximum interaction with the local population, thereby maximizing the pool of potential sources of information. The HCT must be integrated into the supported unit's ISR plan and be provided with other command elements as needed to support the collection mission. The team leader will advise the supported unit on the specific capabilities and requirements of the team to maximize mission success. This method also increases the risk to the team. HCT members must carry the necessary firepower for self-protection. They must also have adequate communications equipment to call for help if needed. The team's posture, equipment, and appearance will be dictated by overall force restrictions and posture. When operating as an independent patrol, the HCT should not stand out from overall US forces operations. If US forces are in battle-dress uniforms and operating out of military vehicles, so should the HUMINT collectors.
- Soft. If the threat situation is such that soldiers are authorized to wear civilian clothes when outside base areas, the HUMINT collectors should also move among the civilian population in civilian clothes, so that they do not stand out from others in the area.

CIVIL SUPPORT OPERATIONS

3-15. Army support supplements the efforts and resources of state and local governments and organizations. If a presidential declaration initiates civil support for a major disaster or emergency, involvement of DOD intelligence components would be by exception. Civil support requires extensive coordination and liaison among many organizations—interagency, joint, AC, and RC—as well as with state and local governments, and in any case will require compliance with the Posse Comitatus Act, 18 U.S.C., § 1385, when US forces are employed to assist Federal, state, or local law enforcement agencies (LEAs). The National Response Plan provides a national level architecture to coordinate the actions of all supporting agencies.

MILITARY OPERATIONS IN URBAN ENVIRONMENT

3-16. Units are often task organized with additional ISR units and assets to meet the detailed collection requirements in the urban operations. The complexities of urban terrain cause degradation in the capabilities of many of the sensor systems. HUMINT collectors may have to be placed in DS of lower echelon combat maneuver forces (battalion and lower) to support operations. HUMINT and combat reporting by units in direct contact with threat forces and local inhabitants becomes the means of collection. For successful ISR

planning, the S2 must be aware of the capabilities and limitations of the various organic and attached collection systems as they apply to urban operations. As in all environments, commanders must assess the risk involved in the forward deployment of HUMINT assets.

3-17. In urban operations, people (for example, detainees and civilians) are the preeminent source of information. HUMINT collection provides information not otherwise available through signals intelligence (SIGINT) and imagery intelligence (IMINT) such as threat and local population intentions. They collect information on, for example, floor plans, defensive plans, locations of combatants and noncombatants, including civilians in the buildings and surrounding neighborhoods, and other information. The collected information is passed directly to the individuals conducting the combat operation.

3-18. In small-scale contingencies (SSCs) and in peacetime military engagements (PMEs), contact with local officials and populace by the HUMINT collectors can be a prime source of information about the local environment and is a vital component of intelligence support to force protection. During routine patrolling of urban areas it is often expedient to place a HUMINT collector with individual patrols. The key difference between urban and other operations, from major theater war (MTW) to PME, is the number of HUMINT collectors required. The need for HUMINT collectors is a function of population density. Whereas in a rural environment, a HUMINT team may be able to cover an area in excess of 1,200 square kilometers; the same team in a dense urban environment may be able to cover only 10 square blocks or less.

HUMINT COLLECTION ENVIRONMENTS

HUMINT COLLECTION IN A PERMISSIVE ENVIRONMENT

3-19. In a permissive environment, HCTs normally travel throughout their specific AOR as separate teams or as part of a larger reconnaissance team. HUMINT collectors may frequently make direct contact with the individual, view the activity, or visit the area that is the subject of the ISR effort. They normally use debriefing and elicitation to obtain first-hand information from local civilians and officials as their primary collection techniques. Additional information can be obtained from exploitation of open-source material such as newspapers, television, and other media. The priority requirements in this environment are normally linked to force protection. HCTs should establish liaison and casual source contacts throughout their AOIR. Reporting is normally via IIRs, although SALUTE reports are used for critical time-sensitive reporting. Even in a permissive environment, the HUMINT collector conducts the majority of his collection through the debriefing of individuals who have first-hand knowledge of the information they are reporting.

HUMINT COLLECTION IN A SEMI-PERMISSIVE ENVIRONMENT

3-20. In a semi-permissive environment, security considerations increase, but the risk to the collector still must be weighed against the potential intelligence gain. HCTs should still be used throughout their AOIR but will normally be integrated into other ground reconnaissance operations or other planned operations. For example, a HUMINT collector may accompany a CA team or PSYOP team visiting a village. Security for the team and their sources is a prime consideration. The HCTs are careful not to establish a fixed pattern of activity and arrange contacts in a manner that could compromise the source or the collector. Debriefing and elicitation are still the primary collection techniques. Teams are frequently deployed to conduct collection at roadblocks, refugee collection points, and detainee collection points. They may conduct interrogations of EPWs and other detainees within the limits of the mission-specific orders, and applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. DOCEX is also used to accomplish exploitation of threat documents. Reporting is normally via SALUTE report and IIR.

HUMINT COLLECTION IN A HOSTILE ENVIRONMENT

3-21. In a hostile environment, the three concerns for HUMINT collection are access to the sources of information, timeliness of reporting, and security for the HUMINT collectors. Prior to the entry of a force into a hostile AO, HUMINT collectors are used to debrief civilians, particularly refugees, and to interrogate EPWs and other detainees who have been in the AO. HCTs are normally located with the friendly units on the peripheries of the AO to facilitate timely collection and reporting. If a refugee or EPW/detainee population exists prior to this mission, they are screened to determine knowledgability of the AO and are debriefed or interrogated as appropriate. HUMINT collectors accompany the friendly ground reconnaissance elements as they enter the AO. As part of the ground reconnaissance force, they interrogate EPWs and other detainees and debrief refugees, displaced persons, and friendly force patrols. Reporting is normally via oral or written SALUTE reports with more detailed information reported via IIRs. They may also support the S2 through the systematic debriefing of friendly ground reconnaissance assets and the translation of any documents collected by them.

EAC HUMINT

MI BRIGADES AND MI GROUPS SUPPORTING COMPONENT COMMANDS

3-22. Each SCC with an outside continental United States (OCONUS) responsibility has an US Army Intelligence and Security Command (INSCOM) MI brigade or group to provide operational HUMINT support to that command. These MI elements provide peacetime support to the unified

command and add a consistent, forward-deployed presence in a particular theater of operations. Theater MI brigade and group assets provide HUMINT support during contingency operations. These HCTs can support a JTF, an army combatant command, or any deployed element that requires augmentation.

JOINT, COMBINED, AND DOD HUMINT ORGANIZATIONS

3-23. The Departments of the Air Force and the Navy have limited HUMINT collection capability. They will normally provide strategic debriefing trained and certified personnel to joint interrogation and debriefing facilities primarily to collect information on areas of particular interest to that Military Department. Within the Department of the Navy, however, the US Marine Corps has a robust tactical HUMINT collection capability that operates primarily in support of engaged Marine Corps forces. Marine expeditionary elements deploy with human exploitation teams (HETs) that provide organic HUMINT and CI support to the deployed Marine force. Marine HETs are rapidly deployable and fully equipped to conduct the full range of tactical HUMINT and CI functions. They can provide support to either the deployed Marine force or as part of JTF HUMINT or CI teams. Each Marine Expeditionary Force (MEF) has organic HETs. HETs can also be attached to a Marine Air-Ground Task Force (MAGTF) for a particular operation.

SUPPORT AGENCIES

3-24. HUMINT agencies from DOD, national level intelligence agencies, and LEAs can support the battlefield commander. In a JTF, a national intelligence support team (NIST) works with the J2X to coordinate national level activities with JTF and component HUMINT and analytical assets. Sometimes liaison officers (LNOs) are assigned directly to the C/J/2X to facilitate collection activities.

- **Defense Intelligence Agency (DIA).** The DIA is a DOD combat support (CS) agency and an important member of the United States Intelligence Community. With more than 7,000 military and civilian employees worldwide, DIA is a major producer and manager of foreign military intelligence. DIA provides military intelligence to warfighters, defense policymakers and force planners in DOD and the Intelligence Community in support of US military planning and operations and weapon systems acquisition.
 - **Defense HUMINT (DH) Service.** The DH Service, a branch of the DIA, is the force provider for strategic HUMINT forces and capabilities. During operations, elements from DH form a partnership within the supported JTF headquarters J2X element for the coordination and deconfliction of HUMINT source-related collection activities. DH support to a joint force is outlined in the classified DIAM 58-11 and DIAM 58-12.
- **Central Intelligence Agency (CIA).** The CIA supports US national security policy by providing accurate, evidence-based, comprehensive, and timely foreign intelligence related to national security. The CIA

conducts CI activities, HUMINT collection, special activities, and other functions related to foreign intelligence and national security as directed by the President. Joint Pub 2-01.2 (S//NF) contains details of CIA contributions to the deployed force.

- **Department of State.** The State Department's Bureau of Diplomatic Security provides CI support to diplomatic missions worldwide and gathers extensive information on intelligence capabilities of adversaries within that diplomatic mission's area of concern. The Bureau of Intelligence and Research is the State Department's primary source for interpretive analysis of global developments. It is also the focal point in the State Department for all policy issues and activities involving the Intelligence Community.
- **National Security Agency (NSA).** The NSA is a DOD agency that coordinates, directs, and performs highly specialized activities to protect US information systems and produce foreign intelligence information. It is also one of the most important centers of foreign language analysis and research within the Government.
- **Defense Criminal Investigative Service (DCIS).** The DCIS is the criminal investigative arm of the Inspector General (IG) of DOD. The DCIS's mission is to protect America's warfighters by initiating, conducting, and supervising investigations in support of crucial National Defense priorities.
- **Department of Justice**:
 - Federal Bureau of Investigation. The FBI may provide the deployed commander with national level expertise on criminal and CI issues if currently operating in a task force (TF) AO and liaison is established early.
 - Drug Enforcement Agency (DEA). The DEA provides counterdrug operational expertise to a deployed TF and coordinates its operations with those of a deployed TF.
- **Department of Homeland Security (DHS).** The DHS mission is to prevent terrorist attacks within the United States, reduce the vulnerability of the United States to terrorism, protect the homeland, its citizens, and critical infrastructure and key resources against terrorist attack. DHS provides a lead for Federal incident response, management, and recovery in the event of terrorist attack and natural disasters. The Secretary of Homeland Security is the principal Federal official for domestic incident management. Pursuant to the Homeland Security Act of 2002, the Secretary is responsible for coordinating Federal operations within the United States to prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies. DHS operates the Homeland Security Operations Center (HSOC) and the DHS-led Interagency Incident Management Group (IIMG). The DHS AOR is the US and its territories. DHS secures and protects the entry points to the nation, the areas between the entry points, land and water, for people, and cargo or conveyances. DHS enforces immigration, customs, and transportation security laws and

regulations, counter-narcotics, counterfeiting, financial crimes, and threats to the President. As legislated in the Homeland Security Act of 2002, DHS is chartered as the primary outreach Federal activity for state, local, and tribal governments, and the private sector. Although DHS has no direct role in support of a "battlefield commander" outside the United States, DHS component organizations have representatives deployed in support of US Government missions in the US Central Command (USCENTCOM) AOR.

- **Department of Energy (DOE).** The DOE can assist with the—
 - Exploitation of weapons of mass destruction (WMD).
 - Protection or elimination of weapons and weapons-useable (dual-use) nuclear material or infrastructure.
 - Redirection of excess foreign weapons expertise to civilian enterprises.
 - Prevention and reversal of the proliferation of WMD.
 - Reduction of the risk of accidents in nuclear fuel cycle facilities worldwide.
 - The capability enhancement of WMD detection including nuclear, biological, and chemical (NBC).
- **National Geospatial Intelligence Agency (NGA).** The NGA is a member of the US Intelligence Community and a DOD Combat Support Agency. NGA provides timely, relevant, and accurate geospatial intelligence in support of national security objectives. Geospatial intelligence is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth.
- **Counterintelligence Field Agency (CIFA).** The mission of CIFA is to develop and manage DOD CI programs and functions that support the protection of the Department. These programs and functions include CI support to protect DOD personnel, resources, critical information, research and development programs, technology, critical infrastructure, economic security, and US interests against foreign influence and manipulation, as well as to detect and neutralize espionage against the Department.

3-25. Most potential coalition partners have some type of HUMINT capability. Less developed nations may use HUMINT as their primary collection system and may be quite skilled in HUMINT operations. These assets will be present on the battlefield, and US assets are likely to work with them. HCTs should perform regular liaison with coalition HUMINT personnel. It is likely that some coalition partners will be more knowledgeable of the culture in the AO and be able to share insights with US HCTs.

Chapter 4

HUMINT Operations Planning and Management

4-1. HUMINT operations planning and management are supported by a robust structure that includes staff elements such as the C2X when working with non-US forces at the Joint intelligence staff level, G2X at the Division, Corps intelligence staff, the HUMINT operations section in the MI Battalion, and HAT in the Division and Corps ACE. It also includes C2 elements at the MI battalion, company, platoon, and team levels. The OMT provides the first level of staff and C2 functions when two or more HCTs deploy in support of an operation. (See Table 4-1.)

Table 4-1. HUMINT Operations.

ECHELON	ISR PLANNING	TECHNICAL SUPPORT AND DECONFLICTION	MISSION EXECUTION
COMBINED	C2/ACE	C2X/OMT	MI CDR
JOINT	J2/ACE	J2X/OMT	MI CDR (AMIB or MI Battalion)
CORPS/DIVISION	G2/ACE	G2X/OMT	MI CDR/OMT
BRIGADE	S2	MI CDR/OMT	MI CDR/OMT

HUMINT AND THE OPERATIONS PROCESS

4-2. Following the operations process defined in FM 3-0, Chapter 6, there are four components within HUMINT operations: Plan, Prepare, Execute, and Assess.

PLAN

4-3. HUMINT planning defines collection objectives, when to collect it, and which resources will be tasked to do the collection. Commanders with HUMINT collection assets in their units receive collection tasking based on requirements developed during ISR planning. The commander and staff, in concert with their supporting OMTs, assess the requirements and task the team or teams best capable of answering the requirement based on contact placement and access.

4-4. Another aspect to consider carefully during the Plan phase of the operational cycle is technical control. Technical control is ensuring adherence to existing policies and regulations, providing information and guidance of a technical nature, and supervising the MOS-specific TTP required in

conducting collection missions. Planning must take into account that technical control does not interfere with or supersede any C2 that a commander has over an asset or unit nor does it interfere with collection of the commander's requirements. For HUMINT collectors, the technical control network includes the C/J/G/S2X, the HOC, and OMTs. Technical control includes the management of source and other sensitive data and databases, the management of intelligence contingency and incentive funds, the liaison with other HUMINT organizations, and the deconfliction of operations. Technical control provides HCTs with specific requirements and data that they need to conduct operations and, in certain circumstances, specific instructions on how to execute missions.

PREPARE

4-5. During this phase, commanders and staff, including HUMINT management sections, review HUMINT mission plans. This review is to ensure all areas of the mission are considered and addressed in the plan and included in rehearsals. Items to cover include but are not limited to—

- Route (primary and alternate).
- Communications.
- Security plan.
- Convoy procedures including actions on contact and rally points.
- Initial requirements to be covered.
- Mission duration.

4-6. The HUMINT collector then researches the topic area addressing the requirement and prepares a questioning plan. The HCTs and OMTs must coordinate all mission requirements. It is important that HUMINT elements are included in all rehearsals conducted by their supported unit. These rehearsals will enable HCTs to carry out essential coordination with other units and ensure that they are included in and familiar with procedures such as resupply, communications, casualty evacuation, fire support, and fratricide avoidance. Rehearsals and briefbacks will allow the supported command to see and correct problems with their support to the HUMINT elements prior to deployment.

EXECUTE

4-7. Mission execution consists of the collection of information in accordance with the integrated ISR plan. The requirements manager validates the requirements based on command guidance. The G3 tasks the requirements to the units and the individual asset managers (that is, OMT) to identify the assets best capable to answer the requirement. When requirements are levied against a specific HCT, the HCT leader decides which of his team's contacts can best answer the requirements. He then turns the requirement into specific team tasks.

ASSESS

4-8. Assessment is the continuous monitoring—throughout planning, preparation, and execution—of the current situation and progress of an

operation, and the evaluation of it against criteria of success to make decisions and adjustments. Assessment plays an integral role in all aspects of the intelligence process (see FM 2-0).

HUMINT COMMAND AND CONTROL

4-9. Commanders of organizations that conduct HUMINT operations are responsible for task organization, mission tasking, execution, mission accomplishment, and designation of subordinate AOs (within the guidelines of the OPORD or OPLAN**).** MI unit commanders who exercise direct control of HUMINT operations, including interrogation operations, at all levels are responsible for and stand accountable to ensure HUMINT collection activities comply with this manual and applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. The MI unit commanders must ensure mission accomplishment by properly allocating resources and logistics in support of all HUMINT collection assets assigned to their units. Commanders must ensure that their HUMINT collection personnel are trained and ready for the mission. There is a need for a partnership between the J/G2X, who exercises technical direction and oversight responsibility and the MI commander, who exercises direct command authority and responsibility. The MI unit commander analyzes the higher headquarters mission, concept of operations, and the specified and implied tasks given to his unit. He restates the unit mission, designs the concept of operations, task organizes his assets, and provides support to subordinate units. Specifically, the MI unit commander—

- Issues mission orders with sufficient details and time for subordinate commanders and leaders to plan and lead their units.
- Must know the threat, his organization, ISR systems, counter-ISR systems, operations, and terrain over which his units will operate and how that terrain enhances or limits HUMINT collection operations.
- Must be aware of the operational and technical limitations of his unit and ensures that all assets are task organized, properly positioned, and fully synchronized to accomplish the mission.
- Oversees the collective and individual training within his unit.
- Coordinates continuously with the higher headquarters staff, the supported maneuver unit staff, and other commanders to ensure integrated R&S operations and support.
- Establishes clear, consistent standards and guidance for current and future operations in order to adhere to policy and the higher headquarters commander's intent without his constant personal supervision.
- Continually assesses his unit's ability to sustain its internal operations and its ability to support assigned missions and keeps the higher headquarters staff informed of unit, equipment, and personnel status that affect collection operations.

- Advises his higher headquarters commander and staff on the capabilities, limitations, and most effective employment of his assets.
- Remains flexible during operations to adjust or execute missions upon receipt of new orders and when the situation changes.
- Ensures personnel are working within legal, regulatory, and policy guidelines.

TECHNICAL CONTROL

4-10. Technical control refers to supervision of the TTP of HUMINT collection. Technical control ensures adherence to existing policies or regulations and provides technical guidance for HUMINT operations. The elements that provide technical control also assist teams in translating collection requirements into executable tasks. Commanders rely on the expertise of intelligence personnel organic to their unit and within higher echelons to plan, execute, and assess the HUMINT collection effort. The OMTs, HATs, and the HOC of the C/J/G/S2X provide technical control. They—

- Define and manage operational coverage and direction.
- Identify critical collection criteria such as indicators associated with targeting.
- Prioritize collection missions in accordance with collection requirements.
- Advise teams on collection techniques and procedures in accordance with policy, regulations, and law.
- Register and deconflict sources.
- Conduct operational reviews.
- Advise commanders.
- Conduct operational coordination with staff elements and other intelligence agencies.
- Manage ICF and incentive usage.

COMMAND AND SUPPORT RELATIONSHIPS

4-11. The activities of HUMINT assets are governed by their command or support relationship. There are subtle differences in the Joint versus the Army description of some of the command and support relationships. Tables 4-2 through 4-4 show these relationships.

4-12. During interrogation operations, close coordination must occur between intelligence personnel and personnel responsible for detainee operations including MP security forces, Master at Arms, and other individuals providing security for detainees. The facility commander is responsible for all actions involving the humane treatment, custody, evacuation, and administration of detainees, and force protection. Whereas, the intelligence commander is responsible for the conduct of interrogation operations.

COMMAND AND SUPPORT RELATIONSHIPS FOR HUMINT OPERATIONS

4-13. Clear command and support relationships are fundamental in organizing for all operations. These relationships identify responsibilities and authorities among subordinate and supporting units. The commander designates command and support relationships within his authority to weight the decisive operation and support his scheme of maneuver. Some forces available to a commander are given command or support relationships that limit his authority to prescribe additional relationships. Command and support relationships carry with them varying responsibilities to the subordinate unit by parent and gaining units. By knowing the inherent responsibilities, a commander may organize his forces to establish clear relationships.

4-14. Command relationships establish the degree of control and responsibility commanders have for forces operating under their tactical control (TACON). When commanders establish command relationships, they determine if the command relationship includes administrative control (ADCON). Table 4-2 shows Army command and support relationships and Table 4-3 shows joint command relationships chart from FM 3-0 (derived from JP 0-2 and JP 3-0).

4-15. Support relationships define the purpose, scope, and effect desired when one capability supports another. Support relationships establish specific responsibilities between supporting and supported units. Table 4-2 shows Army command and support relationships and Table 4-4 shows joint support relationships from FM 3-0 (derived from JP 0-2 and JP 3-0).

HUMINT REQUIREMENTS MANAGEMENT

4-16. The G2/S2 is responsible for RM. He uses the requirements management (RM) process to orchestrate the actions of the unit's organic and supporting ISR capabilities into a unified effort to gain situational understanding and answer the commander's PIRs. Through centralized planning and decentralized execution, RM optimizes the integration of ISR operations into the commander's scheme of maneuver and fire and into the unit's long- and short-range planning. Control mechanisms within the RM structure facilitate the identification of information shortfalls and the redirection of ISR assets to new intelligence production, reconnaissance, or surveillance missions.

Table 4-2. Army Command and Support Relationships.

IF RELATIONSHIP IS:		INHERENT RESPONSIBILITIES ARE:							
		Has Command Relationship with:	May Be Task Organized by:	Receives CSS from:	Assigned Position or AO By:	Provides Liaison To:	Establishes/ Maintains Communications with:	Has Priorities Established by:	Gaining Unit Can Impose Further Command or Support Relationship of:
COMMAND	**Attached**	Gaining unit	Gaining unit	Gaining unit	Gaining unit	As required by gaining unit	Unit to which attached	Gaining unit	Attached; OPCON; TACON; GS; GSR; R; DS
	OPCON	Gaining unit	Parent unit and gaining unit; gaining unit may pass OPCON to lower HQ. Note 1	Parent unit	Gaining unit	As required by gaining unit	As required by gaining unit and parent unit	Gaining unit	OPCON; TACON; GS; GSR; R; DS
	TACON	Gaining unit	Parent unit	Parent unit	Gaining unit	As required by gaining unit	As required by gaining unit and parent unit	Gaining unit	GS; GSR; R; DS
	Assigned	Parent unit	Parent unit	Parent unit	Gaining unit	As required by parent unit	As required by parent unit	Parent unit	Not Applicable
SUPPORT	**Direct Support (DS)**	Parent unit	Parent unit	Parent unit	Supported unit	Supported unit	Parent unit; Supported unit	Supported unit	Note 2
	Reinforcing (R)	Parent unit	Parent unit	Parent unit	Reinforced unit	Reinforced unit	Parent unit; reinforced unit	Reinforced unit: then parent unit	Not Applicable
	General Support Reinforcing (GSR)	Parent unit	Parent unit	Parent unit	Parent unit	Reinforced unit and as required by parent unit	Reinforced unit and as required by parent unit	Parent unit; then reinforced unit	Not Applicable
	General Support (GS)	Parent unit	Parent unit	Parent unit	Parent unit	As required by parent unit	As required by parent unit	Parent unit	Not Applicable

NOTE 1. In NATO, the gaining unit may not task organize a multinational unit (see TACON).

NOTE 2. Commanders of units in DS may further assign support relationships between their subordinate units and elements of the supported unit after coordination with the supported commander.

Table 4-3. Joint Command Relationships and Inherent Responsibilities.

(from FM 3-0, derived from JP 0-2 and JP 3-0)

Inherent Responsibilities Are:	If relationship is:		
	COCOM	OPCON	TACON
Has command Relationship with:	Gaining combatant commander; gaining service component commander	Gaining Command	Gaining Command
May be task organized by:	Gaining combatant commander; gaining service component commander	Gaining Command	Parent Unit
Receives logistic support from:	Gaining service component commander	Service component command; parent unit	Parent Unit
Assigned position or AO by:	Gaining component commander	Gaining Command	Gaining Command
Provides liaison to:	As required by gaining component commander	As required by gaining command	As required by gaining command
Establishes and maintains communications with:	As required by gaining component commander	As required by gaining command	As required by gaining command and parent units
Has priorities established by:	Gaining component commander	Gaining Command	Gaining Command
Gaining unit can impose further command relationship/authority of:	OPCON; TACON; direct support; mutual support ; general support; close support	OPCON; TACON; direct support; mutual support; general support; close support	Direct support; mutual support; general support; close support

Table 4-4. Joint Support Categories.

(from FM 3-0, derived from JP 0-2 and JP 3-0)

CATEGORY	DEFINITION
General Support	The action given to the supported force as a whole rather than to a particular subdivision thereof.
Mutual Support	The action that units render each other against an enemy because of their assigned tasks, their position relative to each other and to the enemy, and their inherent capabilities.
Direct Support	A mission requiring a force to support another specific force and authorizing it to answer directly the supported force's request for assistance.
Close Support	The action of the supporting force against targets or objectives that are sufficiently near the supported force as to require detailed integration or coordination of the supporting action with fire, movement, or other actions of the supported force.

DEVELOP HUMINT REQUIREMENTS

4-17. The first step in the RM process is to develop intelligence requirements that accurately identify and prioritize the commander's concerns about the threat and the battlefield environment that must be resolved to accomplish the mission. The G2/S2X, or his representative, normally supports the G2/S2 by identifying HUMINT collection requirements and opportunities and advises the command and staff on HUMINT capabilities. The HUMINT representative must be able to discuss any delays or risks involved in using HUMINT assets. Through participation in the requirements development process, the HUMINT representative has a thorough understanding of the commander's intent and concept of operations and is better able to support the overall ISR effort.

4-18. The analysis of HUMINT requirements is normally a coordinated effort between the HUMINT and CI staff officer (C/J/G/S2X) and the HAT of the supporting analysis element. The C/J/G/S2X team—

- Records all HUMINT requirements whether generated internally (Specific Orders) or received from other echelons or units (Requests).
- Tracks each requirement from receipt to final satisfaction.
- Reviews each requirement for its—
 - **Feasibility.** Feasibility is a determination if a requirement can be answered given available time and resources.
 - **Completeness.** Does the requirement contain all the specifics needed for collection, such as: What the collection requirement is? When the latest time information is of value (LTIOV)? Why it needs to be collected? Who needs the results of the collection?
 - **Necessity.** The C/J/G/S2X team, with the assistance of the HAT, checks available intelligence databases to determine if the required

information has already been collected or is included in an intelligence product.

4-19. The RM team, with the assistance of the C/J/G/S2X team and the HAT, breaks the HUMINT-related PIR into SIRs. Each SIR describes the indicator of threat activity linked to an area or specific location and time. The HOC evaluates—

- Reportable criteria that are linked to the threat activity. The HOC associates these characteristics with a SIR, and compares the characteristics to a particular HUMINT asset's capability to collect.
- Range, which is the distance from the current location of the HUMINT asset or resource to the source. In other words, are there sources available that had or have access to relevant information on the area or activity in question, and can the HUMINT team contact them in a timely manner?
- Timeliness, which is when the information must reach the commander to be of value; that is, the LTIOV.

4-20. The RM team, supported by the C/J/G/S2X and the HAT, attempts to answer the SIRs with intelligence products developed from information available within the existing intelligence databases or pulled from other organizations within the intelligence architecture. If the requirement can be answered in this manner, the intelligence is immediately disseminated. When the required information is neither available nor extractable from archived information or from lower, lateral, or higher echelons, the C/J/G/S2X team develops it into an RFI to higher or an ISR tasking for organic or attached HUMINT assets. The compilation of unanswered requirements and how to answer them form the basis of the ISR plan. The tasking may be in the form of an SDR. An SDR is a specific request or tasking for a collector to question a source on a particular collection requirement. This request involves analysis that results in the conclusion that a specific source possibly has the placement and access to answer a SIR. SDRs are specific; whereas, HUMINT collection requirements (HCRs) are general.

DEVELOP THE HUMINT PORTION OF THE INTEGRATED ISR PLAN

4-21. The HOC within the C/J/G/S2X section assists the G3/G2 in developing the HUMINT portion of the ISR plan in coordination with the HAT and the RM team. The HOC ensures that the HUMINT capabilities and taskings are included in the plan although the plan often will not contain the specifics of HUMINT operations due to the sensitivity of the sources and techniques. The HOC will coordinate with the Office of the SJA to ensure the HUMINT portion of the integrated ISR plan complies with applicable law and policy prior to its implementation. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. The HOC coordinates with C/J/G/S2X for mission deconfliction at that echelon to specify the collection capability and current

status of the various HUMINT organizations to better enable him to select the "best" organization to collect on various SIRs. HUMINT collection generally requires time to develop the environment and access sources.

4-22. The HUMINT collection environment during an SSC is different from an MTW. During an MTW where the force is moving, a division normally plans 48 hours out; a corps plans 72 hours out. In contrast, the planning focus for units supporting an SSC may be 3 to 6 months out. The longer HCTs are in an area, the better the collector is able to develop leads to answer collection requirements. Requirements may be continuous or may be concerned with specific upcoming events such as national elections. HUMINT is a key asset to determine adversary intentions; however, it is highly dependent on the ability to cultivate or locate sources with the desired information. HUMINT in support of stability and reconstruction operations is not a short-term undertaking. [Example: National level elections are taking place in the AO in 3 months. As a part of integrated ISR planning, an assessment must be conducted to determine the capability to answer post-election collection requirements based upon current contacts and HUMINT leads. If there are no leads or contacts that could answer election-related collection requirements, it is necessary to spot, assess, and contact sources to meet requirements.]

4-23. A second part of the HUMINT portion of the integrated ISR plan is the HUMINT collection focus, which—

- Designates which collection requirements comprise the emphasis for collectors' missions.
- Prioritizes collection requirements based upon the operational environment in the AO and future missions in the AO.
- Includes future operational collection tasks which aid in causing a gap or pause in collection as the unit transitions to the next operational phase or the next operation.

4-24. In addition to specific requirements, a statement of intelligence interest (SII) at the joint level or a collection emphasis message at division or corps is issued to identify the overall collection goals for a time period. As the collection request or requirement is passed down, each echelon performs additional planning for its own specific requirements.

Evaluate HUMINT Resources

4-25. After identifying the SIRs, the HOC and the C/J/G/S2X determine the availability and capability of HUMINT assets and resources that might contribute to requirement satisfaction and which are most suited to collect against each SIR. This does not necessarily imply that the C/J/G/S2X assigns a tasking to a specific team; rather, it develops the requirements or requests for an organization that then executes the mission. The HOC and C/J/G/S2X should also consult the HAT for its analysis of additional potential HUMINT assets and resources which might be available, both on and off the battlefield, to contribute to requirement satisfaction. For example, the HAT may be aware of a group of émigrés now living elsewhere who previously lived near a target site, and who might be able to provide answers to collection requirements if debriefed.

Determine Asset or Resource Capabilities

4-26. The HOC translates the capabilities and limitations of the available HUMINT assets into a set of factors that they can compare to the SIR characteristics. Asset capability factors are technical or performance characteristics, location, and source access. Each HUMINT asset is evaluated for its—

- **Availability.** The HOC reviews the list of viable HUMINT assets for current availability and the addition or deletion of capabilities. This includes considerations such as maintenance time and previous taskings. Coordination with adjacent and higher headquarters and national level agencies by the C/J/G/S2X will determine the availability of higher echelon resources.
- **Survivability**. Survivability must be commensurate with the threats to which the HUMINT assets will be exposed during the course of operations. These assets must be as survivable as, or in certain circumstances more survivable than, the forces they support. The HOC and the commander must weigh the risk versus the gain in using HUMINT assets.
- **Reliability.** Reliability is the ability of the asset to overcome threat deception measures such as misinformation or false information. In HUMINT there are two areas of reliability: source and collector. Source reliability is the determination on the part of the collector if the source is providing accurate information. Collector reliability is a determination on the part of the HOC that the HUMINT collectors within a particular organization have the level of training and experience to collect against a given requirement.
- **Suitability**. Tasking must be based on an asset's capability and on its suitability within the context of the overall plan. For example, HUMINT assets may be capable of collecting against a single target but have unique capabilities against a second target. Intelligence requirements may necessitate tasking these HUMINT assets against the second target if other assets can maintain adequate coverage of the first target.
- **Connectivity.** Connectivity is a critical aspect of any R&S operation. Interoperability, reliability, and robustness of sensors, communications, and supporting automated data processing (ADP) are crucial to the responsiveness, survivability, and overall combat effectiveness of a HUMINT asset. If the automation and communications systems of a HUMINT asset are dissimilar to those of other units in the AO, or if connectivity among assets, supporting systems, and supported systems and elements is too fragile to withstand the stress of operations, commanders will be deprived of important information essential to conducting tactical operations. The HUMINT asset must be able to transmit accurate and timely information to those who must receive it when they need it. Report formats should adhere to established standards in order to ensure that information is easily retrieval at the user desktop through automated queries (push/pull). Planners must look carefully at systems compatibility and the degree of interoperability among the components

of the communications architecture. The better the interoperability of assets and the more robust and redundant the communications links, the better the cross-cueing and analytical exchange.

Develop the Scheme of Support

4-27. The scheme of support is the orchestration of HUMINT assets, resources, and requirements to facilitate the collection of information most effectively. It includes all assets that the G3/S3 can task (organic, attached, and DS) and the G2 can request (from higher or adjacent units). By reviewing available HUMINT assets and higher echelon resources, the HOC and the G/S2X determine whether unit assets or higher echelon resources are best able to answer the requirements. If another echelon can answer an SIR, then the J/G/S2, normally through the C/J/G/S2X, requests them to collect the information and deliver the intelligence product. When planning the HUMINT portion of the ISR plan, the HOC should consider the following:

- **Cueing** is using one asset to tip off another to a possible target. The HOC should look for opportunities for HUMINT assets to cue other collection assets and vice versa.
- **Asset redundancy** uses a combination of the same type of assets against a high-priority collection target. This is vital in HUMINT collection since, in dealing with human sources, the information collected is often part of the overall picture or is influenced by the perception and prejudice of the source. The collection on the same target from a number of different assets gives a more accurate intelligence picture and is a method to validate source reporting.
- **Asset mix** uses a combination of different types of assets against a high-priority collection target. When the probability of success of one asset to satisfy the requirement completely is lower than acceptable, the use of multiple capabilities of different assets increases the likelihood of success; for example, using SIGINT assets to intercept voice communications while HUMINT assets observe activities. Neither can collect all the available information, but the information collected by both can be fused into a more complete picture. Like asset redundancy, asset mix places greater demands on the limited assets available, both collection and analysis, and has to be clearly justified by the potential intelligence gain.
- **Integration of new requirements** into ongoing missions may make it possible to reduce timelines, make collection more responsive to the request, and decrease cost and risk. This is critical in HUMINT due to the long time that it takes to develop sources. The use of an existing source to answer new requirements often facilitates collection.

Develop and Prioritize Taskings and Requests for Information

4-28. After the G2/S2X and the G2/S2 approve the HUMINT portion of the ISR plan, the HOC develops specific orders to task assets, develop additional assets, and/or requests to seek higher and lateral support and production. Specific taskings or RFIs are tailored to that specific ISR asset's capabilities and limitations. The G2/S2X supports the requirements manager and the G2/S2 in developing and prioritizing HUMINT taskings. The HOC works

with the unit requirements manager to incorporate the HUMINT plan into the overall unit ISR plan and works with the G3/S3 as necessary to help develop OPORDs or FRAGOs to organic or attached ISR units. HUMINT taskings will often include technical data that cannot be passed through normal tasking channels. The HOC will pass that information directly to the applicable HUMINT OMT or unit operations section.

4-29. The HOC and G2/S2X cannot provide operational taskings to a unit for collection. Collection is a stated mission that the commander executes. However, the technical control the HOC can provide as the HUMINT manager affords the J2/G2X the ability to steer and direct collection assets and operations. The MI commander and OMT determine specifically which teams will collect on a given requirement and are responsible for the TTP used. They report on the status and availability of their collection assets. On the HCT level, the team chief determines which sources will be contacted and the details of how the information will be collected from a given source. A specific plan is developed for each source. This plan should—

- Identify the requirement.
- Identify the proposed source.
- Identify questions to be asked during the source meeting.
- Contain an outline of how the meeting should proceed.
- Identify which collector will conduct the source meeting.

4-30. At the HCT level, the senior team member reviews each plan to ensure the proper planning for the collection mission. The plan is a minimum goal for the collection. The collector must be fully aware of the overall collection priorities and be prepared to take advantage of any additional leads.

DIRECT PRODUCTION

4-31. The G2 coordinates intelligence production to provide non-duplicative all-source intelligence products to the commander, staff, and subordinate forces. Some type of production occurs in the intelligence staff or separate analysis element at every echelon from national to battalion level. The HCT of the ACE at echelon's division and higher will support the intelligence production process through the analysis of HUMINT information and the development of single-discipline HUMINT products.

DISSEMINATE INFORMATION

4-32. The 2X element at each level is normally the release authority for HUMINT reporting and products, ensuring that reporting, products, and data are disseminated to the lowest appropriate level. The G/S2X should preplan criteria for the immediate release of combat information on high-value targets, impending attacks, or other time-sensitive requirements. This preplanning will ensure that commanders and other users quickly receive the information in a format that supports situational understanding, strategic responsiveness, and ISR and provides support to effects. Special effort is also made to ensure that information obtained from detainees is passed back down to the unit that detained them. This measure will support the efforts of the commander as well as building trust in the intelligence process.

EVALUATE REPORTING

4-33. The HAT and the HOC provide the requirements manager and the G2/S2 with expertise to support report evaluation. An important part of the evaluation process is providing feedback to the collectors. Feedback is important in HUMINT operations since the same source may be contacted again for additional information. The collector needs feedback on the accuracy, reliability, and appropriateness of the information reported. The G/S2X team tracks reporting to determine how well the HUMINT collection and production efforts are satisfying the PIRs. The G/S2X team supports the RM team's requirements to—

- **Monitor and Maintain Synchronization.** Through coordination with the G2/S2, the G/S2X, and the HAT, the HOC knows when and what critical pieces of information are missing from the commander's estimate of the situation. The HOC uses the HUMINT portion of the ISR plan to ensure synchronization with the overall operation and scheme of maneuver. The other critical tool for the HOC is the decision support template (DST). The HOC must have a complete copy of this document, ensuring the HUMINT assets do not miss a collection requirement.
- **Correlate Reports to Requirements.** The HOC tracks which specific order or group of specific orders originates from which PIR to ensure that the collected information was provided to the original requester. This also allows the HOC to rapidly determine which asset is available for retasking.
- **Screen Reports.** Each report received is screened for accuracy, timeliness, and applicability to the original tasking or request. If the HOC determines that it completely fulfills the tasking or request, the HOC informs the G/S2X and G2/S2 so that the tasking or request can be closed and the information provided to the original requesting unit.
- **Provide Feedback to Collectors and Analysts.** The HOC provides feedback to all the HUMINT R&S assets. This is normally provided through the C2 element of that unit. By doing so, the HOC quickly reinforces if the reporting is answering the original order or request, or the HOC can provide guidance if it is not. This feedback is essential. The RM team may provide additional information on its collection or analysis if the HOC tells the team exactly what is needed or has been missed in the original report.

UPDATE ISR PLAN

4-34. This step aids the G2/G3 in updating the ISR plan by eliminating satisfied collection requirements, redirecting assets to cover non-satisfied requirements, cross-cueing requirements, and adding new collection requirements to the ISR. This process is accomplished by adjusting the HUMINT portion of the overall integrated ISR plan. It maintains intelligence synchronization and optimizes the exploitation of information in response to situation changes in the AO. The updated HUMINT plan is distributed to the G/S2X requirements manager to ensure its incorporation into the overall unit ISR plan. Continuously updating the HUMINT portion of the ISR plan is vital due to the time involved in redirecting HUMINT assets.

HUMINT MISSION PLANNING

4-35. HUMINT mission planning begins when a unit receives a tasking to conduct HUMINT collection in support of a specific mission, operation, or collection plan. The mission analysis portion of the MDMP is explained in FM 5-0. Special factors must be considered when applying the MDMP to HUMINT operations as discussed below.

RECEIVE AND ANALYZE THE HIGHER HEADQUARTERS ORDER

4-36. Attention must be paid to the support relationship (GS or DS) that exists between HUMINT assets and the unit. The operational environment, including applicable law and policy under which the units are operating must be understood, as this affects the ability of the units to perform certain missions. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. Because of frequently overlapping AOIRs in HUMINT operations, other unit missions and potential areas of conflict must be identified. Missions of other non-HUMINT units must be understood for coordination and possible integration of HUMINT assets. The availability of assets from higher echelons, requirements to provide support to lower echelons, and the existence of technical control from higher echelons must be identified. Tasking, reporting, and communications channels must be clearly understood.

ISSUE A WARNING ORDER

4-37. After the commander has analyzed his orders and worked out the mission and related tasks, he must quickly pass on this information to his team. This is accomplished through the WARNO. As a minimum, the WARNO must include to whom the order applies, time and nature of the operation, the earliest time of movement, and the time and place where the OPORD will be issued. Unit members should prepare for movement while the leader is performing the remaining preparatory tasks.

MAKE A TENTATIVE PLAN

4-38. When determining how the mission will be carried out, the commander works with the factors of METT-TC. When planning for HUMINT collection missions, focus must be placed on the human beings (threat, friendly, and neutral) as well as the key terrain on the battlefield, including information on—

- The demographics of both the AO and AOI.
- The organization and structure of all opposition in the AO and AOI.
- The history of the AO and AOI pertinent to the current situation.
- The economic and social data of all groups in the AO and AOI.

- All key leaders (political, military, social, religious, tribal), opinion leaders, and other influences on public opinion.
- The media and its influence on the population of both the AO and AOI.
- The primary and secondary languages and dialects spoken in all parts of the AO.

4-39. A target folder, if one is used, provides valuable up-to-date intelligence information about the AO for mission analysis and planning. Once intelligence products identify the contentious areas, trends, capabilities, and latest issues concerning the AO, the commander may request a target folder prepared on specific items, such as a hostile organization with the inclination and potential to cause harm to friendly forces. Target folders may include—

- Imagery of the AO and personalities.
- Terrain models of the AO.
- Latest information reports from the AO.
- Biographical data on key leaders in the AO.

Review Available Assets

4-40. The commander and staff, including the OMTs or HUMINT operations section, must look at organic assets and consider factors such as language capability, experience in various aspects of collection, analysis, and management. If organic assets are inadequate, the commander and staff should consider additional available assets within the organization and resources from higher echelons. The commander and staff must consider the analysis and management structure of a HUMINT operations section in addition to the OMT and HCTs. During this step the mission analysis and planning group should determine, among other things—

- The number of HUMINT collectors available.
- The number of collectors who are qualified linguists.
- The number of linguists available to support the collectors.
- Force protection considerations.
- The optimal number of HCTs, OMTs, and HUMINT operations sections that can be configured from the available assets.
- Whether additional assets such as CI agents, TECHINT personnel, analysts, additional linguists, or other experts need to be added to some or all the HCTs to meet mission requirements.

Determine Constraints

4-41. This is a critical step in HUMINT mission analysis. HUMINT collection operations are affected by applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. The degree of restriction may depend on the type of operation being conducted. Constraints are normally found in the scheme of maneuver, the concept of operations, and coordinating instructions. Specific to intelligence interrogation operations, in

accordance with DOD Directive 3115.09, "all captured or detained personnel shall be treated humanely, and all intelligence interrogations or debriefings to gain intelligence from captured or detained personnel shall be conducted humanely, in accordance with applicable law and policy. Acts of physical or mental torture are prohibited."

Identify Critical Facts and Assumptions

4-42. The human factor is preeminent in this step. Assumptions and facts include—

- How HUMINT collectors can interact with the local population.
- What types of sources are available.
- What types of adversary intelligence and unconventional threats are present.

Conduct Risk Assessment

4-43. There are inherent risks involved in HUMINT collection. HUMINT collectors need access to the local population to perform their mission. Rules that restrict all forces to base areas to protect the force may be prudent; however, these restrictions can severely degrade HUMINT collection capabilities, particularly in support of force protection requirements. This measure deprives the collectors of sources needed to anticipate and prevent violent incidents. HUMINT collectors receive cultural training as well as security training to allow them to minimize the dangers of interacting with the local population. Commanders must weigh the risk to collectors against the risk to the force as a whole, and determine whether to provide additional security to the HCT in order to allow the team to perform missions outside the base area to gain needed intelligence. DA Pam 385-1 provides guidance for risk assessment.

Select Courses of Action (COAs)

4-44. During COA development the staff, under the commander's guidance, analyzes various options for deploying and implementing HUMINT assets. Input from HUMINT senior NCOs and WOs is vital to COA development and analysis. Items to consider during COA development include—

- The distribution of the HCTs and OMTs within the AO.
- The support relationship (GS and DS) that exists for the deployed teams.
- The command relationship in effect for the HCTs and OMTs (assigned, attached, or OPCON).
- The manner in which the HUMINT assets are phased into the theater.
- The tactical configuration (personnel and equipment) of the HCT.
- The actual number of the HCTs and OMTs and the size of the supporting HUMINT operations section (if any) deployed.
- The priority of the OMT's efforts.
- The priority of linguist support.

COLLECTION PRIORITY

4-45. During the MDMP, the MI commander advises his higher headquarters on the most efficient use of the HUMINT collectors to meet collection requirements. Depending on the particular higher echelon mission and the capabilities of the specific personnel under his command, the supported S2 must decide whether to concentrate collection efforts on source, debriefing, interrogation, tactical questioning, liaison, or DOCEX operations to answer collection requirements. (See Chapter 5 for a description of these operations.) The MI commander may be required by his operational tasking to support any or all of these operations. He must decide how to task organize his assets to meet these requirements. When faced with limited assets, prioritization of collection is paramount.

4-46. A commander normally must prioritize HUMINT collections and DOCEX. Although the decision is primarily dependent on which type of source (human or document) is most likely to give the priority information, other factors such as phase of operation, ROE, source availability, and collection resource capabilities may influence his decision. At the tactical level, both human sources and documents are screened and the senior HUMINT soldier establishes the priorities. If documents and human sources are determined to be equally likely of containing priority information, human sources are normally exploited first due to—

- The ability of the HUMINT collector to get a human source to elaborate and explain his information, which cannot be done with a document.
- The rate at which people forget detailed information.
- The fact that an individual's resistance is easier to bypass immediately after undergoing a significant traumatic experience (capture). Capture thrusts them into an unfamiliar environment over which they have no control and are vulnerable to various approach techniques. This initial vulnerability passes quickly. An individual's established values begin to assert themselves again within a day or two, and the individual's willingness to cooperate might also decrease.

TASK ORGANIZATION

4-47. Because of the need to place HUMINT collectors in contact with the local population and the need in many cases to integrate the HUMINT collection process into other operations, the planning and analysis staff for HUMINT missions is somewhat expanded from the norm. They should include the C/J/G/S2X, SJA, S1, S2, S3, S4, S5, S6, other staff officers, as necessary, Provost Marshal, MP, and US Army Criminal Investigation Command, CA, unit HUMINT commanders, and senior HUMINT technicians of the deploying unit. If the unit's mission is to replace a currently deployed HUMINT unit, a representative of that unit should be included.

4-48. The challenge to the MI commander is the proper training during operations, task organization, placement, and coordination of movement of HUMINT elements to meet collection requirements. The unit modified table of organization and equipment (MTOE) organization, which is designed for an MTW, may have to be modified to meet the specific requirements of

operations in PMEs and SSCs. Augmentation is often needed and must be requested. Task organization must be flexible to adjust to the dynamic mission objectives. Commanders must allow for the augmentation of HCT with other MI specialties and non-MI personnel as mission analysis and planning indicate the need. Mission analysis and planning identify the specific requirements for the HUMINT operations section, HAT, OMTs, and HCTs.

4-49. The composition of the HUMINT elements must be based on METT-TC factors. The number of HCTs and OMTs in the theater depends on the intensity of the collection effort and the geographical coverage of the AO. HCT members should be prepared to support any HUMINT missions they may receive through command channels. They must have the skills to shift easily from one set of functions to another based on the dynamic mission requirements. The number of OMTs in a designated theater will depend on the type and nature of the mission. A single OMT is capable of managing and controlling 2 to 4 HCTs. The size and staffing of the OMT will depend on a number of factors:

- Whether a HUMINT operations section is deployed and how many HCTs are subordinate to it.
- If a single HCT deploys to support a small contingency, there may be no need for an OMT. In this case the team leader must serve as the OMT.
- If three or more OMTs deploy, then a tactical HUMINT operations section should be deployed.
- For every 3 to 4 HCTs and their designated OMT, there should be one headquarters element composed of a platoon leader and a platoon sergeant to handle all administrative and logistical matters.

OPERATIONAL CONSIDERATIONS

RESERVE COMPONENT INTEGRATION

4-50. Given the Army's OPTEMPO and force structure, the integration of RC forces into the AC is highly likely for future operational deployments. Commanders must identify their requirements early and establish proactive coordination (both in garrison and while deployed) with their RC counterparts to fully integrate them during all phases of training and operations. During operations that include significant RC participation, an RC liaison officer normally will be assigned, either temporarily or permanently (at higher echelons), at the appropriate level of command. The commander and staff must ensure that the RC LNO is involved in all aspects of operational planning and execution.

4-51. There are three general categories of RC augmentation:

- Category 1: Formation of specialized units that include a fully integrated AC and RC TOE. The activation of the RC of these units is required for their full operational capability.
- Category 2: Augmentation of active duty units by RC units to fill out unit strength levels or to provide additional functionality. For example, an AC division might require additional HUMINT teams to support it

during a stability operation. If a division required one additional team, it should request a team and not request four HUMINT collectors. If the requirement is for three additional teams, it should request a HUMINT platoon with its organic C2 and OMTs.

- Category 3: The requirement for individual augmentees. This usually occurs when a unit has the C2 structure but needs either additional personnel or additional capability within the command structure. For example, a unit may have a HUMINT platoon but the platoon is at 50 percent strength. Individual augmentation is the easiest method of integration since the individual is integrated in the same manner as any replacement. The augmented unit normally is required to provide all equipment other than initial issue-type equipment.

4-52. There are several items to consider in unit augmentation:

- Accurate Identification of Requirements: During the MDMP, units need to identify those mission-essential capabilities not already present in the unit. The G3/S3, working in conjunction with the G1/S1, considers options that may include RC augmentation of organic units although the final decision to employ RC units is usually determined at Headquarters, Department of Army (HQDA). The requirement for augmentation is forwarded through appropriate personnel channels to US Army Forces Command (FORSCOM) and HQDA, which will identify the appropriate units or personnel. If approved, they will work with the appropriate agencies to establish the timeline in which the units can respond on the Time-Phased Forces Deployment Data List (TPFDDL). When developing requirements, the requesting unit must be sure to articulate its needs accurately, specifying required skills, numbers, and any additional skill identifiers (ASI). [Example: Request augmentation by a HUMINT platoon consisting of at least a platoon headquarters, three HCTs, one OMT, two linguists, and one CI/HUMINT Automated Tool Set (CHATS) proficient operator. The augmenting element will be operating in support of the commander's force protection program in the gaining unit's AOR.]
- Activation Timeline: Units need time to mobilize and conduct any additional collective and individual training that may be specific to the unit's mission or operational environment. The requesting unit needs to be aware of the time required to activate the requested RC and that there may be differences in levels of training or equipment. Timelines should be established by FORSCOM to allow resolution of these problems and should be reflected in the commander's operational planning sequence. Timelines will vary from unit to unit and mission to mission.
- Training: USAR and ARNG units usually cannot train their units or individuals to the same proficiency as the AC. Normally, this is due to the limited amount of training time. Because of this limitation, a certain degree of train-up prior to deployment may be necessary. Commanders should identify available training opportunities and request the participation of personnel identified for augmentation. For an ongoing mission, you should also plan for an extended "right seat

ride" mission handover period once the individuals or unit arrives in the theater of operations.

- Command and Control: If the RC augmentation requires activation of an entire unit, it should include their C2 element. If the augmentation is by individuals, then they will fall under the command and control of the gaining units.
- Time on Active Status: USAR and ARNG soldiers are restricted as to the amount of time they can remain on active status. This timeline begins on the date of mobilization and ends on the day the soldier leaves active duty status. Deployed units must take this into account when conducting continuous operations and must identify the requirement to replace RC forces early enough to allow for the required training and handoff procedures.
- Experience: While RC personnel normally lack current military experience, they often perform jobs in the civilian sector that either mitigate this lack of experience or they are able to bring a new and useful capability with them. Care should be taken that reservists who have civilian jobs which are similar to their HUMINT MOS (such as police officers or investigators) recognize the different constraints under which they operate in the military environment. For example, police officers who might normally task informants with minimal oversight cannot do that in their position as a HUMINT collector. Commanders should try to capitalize on these skills, but ensure proper training and understanding of the policies and regulations that govern HUMINT collection operations.

OPERATIONS PLANS, OPERATIONS ORDERS, AND ANNEXES

4-53. An OPLAN is any plan for the conduct of military operations. When a commander issues a directive for the coordinated execution of a military operation, it becomes an OPORD. Although plans are based on specific conditions or assumptions, they are not static. Plans are changed, refined, and updated as a result of continuous estimates and studies. It is critical to include HUMINT plans in the Intelligence Annex to the OPLAN.

4-54. The OPORD gives the HUMINT element approval to execute its mission. OPORDs define the mission, set the parameters of operations, identify who is responsible for what, and how it is to be supported. Additions that are necessary to amplify an OPLAN or OPORD are contained in annexes, appendices, tabs, and enclosures. Tasking for units to conduct HUMINT collection operations is listed in the main body of the OPORD under **Tasks to Subordinate Units**. The HUMINT appendix to Annex B provides the technical guidance for HUMINT collection including the umbrella concept for HUMINT operations.

4-55. The HUMINT appendices provide details on planning, coordinating, approving, and managing HUMINT operations as they relate to the unit's overall mission. These appendices serve as the basic document authorizing most HUMINT operations and programs. They must be reviewed and approved by the appropriate office or commander. The HUMINT appendix to the ISR Annex is necessary to ensure that augmentation of HUMINT assets

from other components and agencies are integrated throughout the TF as required to facilitate their specialized collection requirements. Specific tabs may include joint debriefing and interrogation facility operations, source operations, DOCEX, or open-source information.

OPERATIONAL COORDINATION

4-56. HUMINT collection is not conducted in a vacuum. Coordination with MI organizations and non-MI agencies, units, and staff organizations is often critical to expedite and complete HUMINT collection operations. (See Appendix C for predeployment planning.)

MI ORGANIZATIONS

4-57. Elements involved in HUMINT planning, execution, and analysis need to maintain close coordination with their counterparts in the other intelligence disciplines. Coordination includes but is not limited to the disciplines shown below.

Imagery Intelligence:

- Support imagery analysis by using HUMINT sources to identify or confirm the identification of items in imagery. This includes, for example, using human sources to identify the functions of buildings that have been tentatively identified through external imagery.
- Coordinate for current military or civilian imagery to use in the questioning of sources.
- Cue requirements managers and others involved in imagery tasking on locations or activities for imagery collection.
- Coordinate for IMINT information to verify information obtained through HUMINT collection.
- Provide imagery for analysis (through still and video photography and captured imagery).
- Coordinate for technical support as required when questioning personnel on subjects related to imagery.
- Obtain imagery-related collection requirements that can be answered by human sources.

Signals Intelligence:

- Support signals analysis by using HUMINT sources to identify or confirm the information obtained through SIGINT collection.
- Coordinate for current SIGINT information to use in the questioning of sources.
- Cue requirements managers and others involved in SIGINT tasking on locations or activities (including communications types and frequencies) for SIGINT collection.
- Coordinate for information to verify information obtained through HUMINT collection.
- Provide SIGINT-related CEDs for SIGINT analysis.

- Coordinate for technical support as required when questioning personnel on SIGINT-related topics.
- Obtain SIGINT-related collection requirements that can be answered by human sources.

Measurement and Signature Intelligence:

- Support measurement and signature intelligence (MASINT) analysis by using HUMINT sources to identify or confirm the information obtained through MASINT collection.
- Cue requirements managers and others involved in MASINT tasking on locations or activities for the location of MASINT sensors.
- Coordinate for information to verify information obtained through HUMINT collection.
- Provide MASINT-related CEDs for MASINT analysis.
- Coordinate for technical support as required when questioning personnel on MASINT-related topics.
- Obtain MASINT-related collection requirements that can be answered by human sources.

Technical Intelligence:

- Support TECHINT analysis by using HUMINT sources and documents to provide information concerning threat equipment and to support TECHINT materiel analysis. This includes, for example, the interrogation or debriefing of equipment operators of the translation of operators manuals for a piece of equipment being investigated.
- Coordinate for current information on equipment capabilities to use in the questioning of sources.
- Cue requirements managers and others involved in TECHINT tasking on locations or activities for TECHINT collection. This includes forwarding the identification and location of equipment of TECHINT interest obtained during HUMINT collection operations.
- Coordinate for TECHINT information to verify information obtained through HUMINT collection.
- Provide information from CEDs in support of TECHINT.
- Coordinate for technical support as required when questioning personnel on subjects related to areas of TECHINT interest.
- Obtain TECHINT-related collection requirements that can be answered by human sources.

Counterintelligence:

- Support CI analysis by using HUMINT sources to provide information concerning adversary intelligence collection capabilities and operations.
- Identify human and document sources that have information of CI interest.

- Cue requirements managers and others involved in CI tasking individuals or activities of CI interest.
- Coordinate for CI information to verify information obtained through HUMINT collection.
- Provide information from CEDs in support of CI.
- Coordinate for CI support as required when questioning personnel on topics related to areas of CI interest.
- Obtain CI-related collection requirements that can be answered by human sources.
- Integrate CI elements into HUMINT collection operations as applicable.

Open-Source Intelligence:

- Support open-source intelligence (OSINT).
- Provide open source maps, charts, phone directories, business directories, newspapers, video and audio media (including tapes and compact discs) to the appropriate J/G/S2X and Intelligence Community agencies and liaison officers.

OTHER ORGANIZATIONS

4-58. In addition to MI units, HUMINT collection organizations frequently conduct coordination with other military organizations.

- **Military Police Units:** Close coordination between HUMINT collectors and MPs is mutually beneficial. The MPs are responsible for maneuver and mobility support, area security, internment and resettlement, law and order, and police intelligence operations. Both activities (HUMINT collection and MP operations) require close contact with the local civilian, refugee, and detainee populations. HUMINT collection at checkpoints and at EPW and other detainee collection points must be coordinated with the MPs, who are normally responsible for internment and resettlement operations. In return, the HUMINT collectors, because of their screening and questioning of these population groups, can help facilitate the MP's population control missions by providing information about the population's activities and intentions that may be of MP concern. At EPW/detainee collection points, HUMINT collectors should arrange with the MP leadership to be allowed to debrief MPs since MPs are in regular contact with the detainees. This does not constitute tasking. Information collected in this manner may provide valuable insight, which can aid the collector in formulating approach strategies. MPs should be debriefed in such a way so as not to interfere with their mission. Liaison with the MP chain of command is vital to gain their support and assure them that HUMINT collection will not interfere with MP operations. Joint patrols containing MPs and HUMINT collectors can also be mutually beneficial in many situations.
- **Criminal Investigation Division (CID) and Provost Marshal Office (PMO):** The goals of HUMINT collection and those of the MPs (particularly CID) are different. CID and PMO are concerned with

identification and apprehension of criminal elements. The goal of HUMINT collection is the collection of information in response to PIRs that in many situations are centered on force protection. In the situation where the threat includes a criminal element, the HCTs might collect OB type information on the criminal element to ascertain their activities and threat to friendly forces. HUMINT collectors are not trained to conduct criminal investigations and must not be used for this purpose. Criminal investigators and HUMINT collectors must carefully coordinate their activities as necessary. HUMINT collectors are required to report to the proper agency information collected on criminal activities that the HUMINT collectors uncover in the normal course of their activities.

- **Psychological Operations Units:** As with the MP force, HUMINT collectors and PSYOP units are often interested in the same target audience but for different reasons. PSYOP units are interested in modifying the target audience beliefs and actions to be more supportive of US goals. Normally, HUMINT collection elements coordinate with PSYOP elements to obtain information concerning the motivational factors and cultural value systems of the individuals to be questioned. PSYOP units, as a part of their normal operations, develop detailed analysis concerning psychological and cultural factors of friendly and hostile elements in the AO. Such information will help HUMINT collection personnel to understand the source's attitude, value system, and perception; it will also help to obtain information more rapidly. At the same time, PSYOP units often will develop collection requirements to determine local attitudes and for information on the effectiveness of PSYOP campaigns. HUMINT collectors can be tasked to collect on these requirements if they are included as PIRs.
- **Civil Affairs Units:** The CA mission often places CA units in contact with the HUMINT collection target audience. If possible, HUMINT collection missions can be established in coordination with CA missions. If the HUMINT collection mission is viewed as having the potential of interfering with the CA mission and coordinated operations are not possible, CA personnel can still be sensitized to intelligence collection requirements and debriefed by HUMINT collectors as part of a friendly force debriefing operation.
- **Drug and Law Enforcement Agency Operations:** Personnel who are employees of DOD intelligence components may be assigned to assist Federal law enforcement authorities and, when lives are endangered, state and local law enforcement authorities; provided such use is consistent with, and has been approved by an official authorized pursuant to DOD Directive 5525.5, Enclosure 4 (reference (i)). Such official shall ensure that the General Counsel of the providing DOD component concurs in such use. Assistance may be rendered to LEAs and security services of foreign governments or international organizations in accordance with established policy and applicable SOFAs, provided that DOD intelligence components may not request or participate in activities of such agencies undertaken against US persons that would not be permitted activities of such components under the procedures of AR 381-10. HUMINT collectors may assist

foreign law enforcement authorities, with prior approval of the J2X. Under no circumstances will HUMINT collectors assist any US or foreign law enforcement authorities in any manner without prior approval by competent authority after a legal review of the proposal.

- **Maneuver Units:** HCTs may be utilized in GS for coverage of an AOIR or in DS to support a specific maneuver unit. The type of coordination needed with maneuver units will vary depending on the type of support relationship the HCT has. HCTs operating in GS should coordinate with maneuver unit commanders when the HCT will be operating in that unit's AO. At a minimum, the HCTs should announce their presence and request information on any conditions or ongoing situations that may affect on the conduct of their mission. An HCT operating in DS of a specific unit will coordinate with the unit for force augmentation to HUMINT patrols as needed in accordance with force protection requirements. The HCT leader should also coordinate with the supported unit's S2 for involvement in debriefings of returning patrol members, checkpoint personnel, convoy leaders and others. HCT leaders may also coordinate to be included in the unit's reconnaissance patrols, as appropriate.
- **Combat Service Support Units:** Current and future combat operations will be conducted in a noncontiguous battlespace. CSS formations and units may be an excellent source for HUMINT collectors. In many situations, DPs and refugees will perceive CSS activities as non-threatening and an activity which can provide them with aid and comfort. CSS operations will naturally draw DPs and refugees hoping to receive support. This could provide opportunities for HUMINT collectors to access this sector of the population. CSS unit S2s should conduct patrol debriefings of returning convoy personnel to capture observations made during convoys, with the goal of cross-cueing the supporting HCT, CI team, or law enforcement element as appropriate.

STAFF COORDINATION

4-59. Successful HUMINT collection operations require support from the staff elements of the supported unit. These elements are collectively responsible for the planning that results in HUMINT tasking. Below is a partial list of the staff responsibilities that affect HUMINT collection:

- G1/S1 HUMINT-related responsibilities include but are not limited to—
 - Supervising the medical support furnished to EPW/detainees.
 - Maintaining a list (by language and proficiency) of qualified linguists within their command.
 - Coordinating with the G4 or G5 for procurement and payment of other interpreters and translators needed to perform intelligence and non-intelligence duties.
 - Ensuring the echelon's OPLAN contains complete provisions for handling and evacuating detainees, refugees, DPs, and local civilians

as required. This plan must satisfy the interests of all other staff officers and provide for—

- Ensuring humane treatment of all personnel.
- Promptly evacuating personnel from the combat zone.
- Integrating procedures for the evacuation, control, and administration of personnel with other combat service (CS) and CSS operations.
- Ensuring delivery of mail to EPWs and other detainees.
- Maintaining detainee (including EPW) statistics.
- Providing administration and control of detainee currency and pay records, including coordinating with appropriate intelligence authorities about investigating large sums of money.

- G2/S2 is responsible for developing intelligence in support of unit operations. The G2/S2 at division and higher and in the interim BCT is supported by a G/S2X and normally a HAT in the performance of his HUMINT-related functions. His HUMINT-related responsibilities include but are not limited to—
 - Obtaining intelligence through intelligence reach to support HUMINT collection.
 - Incorporating HUMINT into the ISR plan.
 - Developing the HUMINT annex to the OPORD and OPLAN.
 - Coordinating to provide technical support for all HUMINT collection operations.
 - Ensuring deconfliction and synchronization for all HUMINT collection assets within the unit's AO. A particular effort must be made to coordinate with all DOD military source operations (MSO), and DOD and other government agencies (OGAs) that may be operating in the AO; with the theater J2X, as part of deconfliction. Failure to deconflict with DOD MSO and OGAs may result in compromise of assets and interruption of collection operations and potentially unintended casualties.
 - Obtaining documents and materials of intelligence interest, including visual and audio media and electronic equipment (such as computers, phones, PDAs) taken from detainees, or seized or loaned, in coordination with the Provost Marshal and other elements.
 - Recording, evaluating, and analyzing collected information and providing feedback to HUMINT collectors.
 - Ensuring adequate HUMINT collection and reporting nets and systems are available.
 - Coordinating with the G3 to ensure plans for HUMINT collection operations are included in unit OPLANs.
 - Coordinating with the G3 to ensure that HUMINT collectors are included in unit training plans, rehearsals, and briefbacks.
 - Drafting instructions for handling, evacuating, and exploiting captured enemy personnel and CEDs. (They coordinate with the G3 to ensure draft instructions are included in the command standing operating procedures (SOPs), OPLANs, and OPORDs.)
 - Projecting capture rates as well as refugee and DP rates.

 - Determining the number of interpreters and translators needed to perform intelligence duties.
 - Coordinating with other agencies and HUMINT collectors for intelligence sharing.
 - Controlling the procedures used to process and grant clearances to the interpreters and translators as required.
 - Coordinating with the civil-military operations (CMO) officer for intelligence screening of local nationals, refugees, and DPs.
 - Coordinating with SJA for legal review of proposed operations.
- G3/S3 is responsible for operations, plans, organization, and training. His HUMINT collection-related responsibilities include but are not limited to—
 - Ensuring the inclusion of HUMINT collection units in the main body of OPLANs and OPORDs under **Tasks to Subordinate Units** and **Task Organization**.
 - Ensuring instructions for handling, evacuating, and exploiting captured enemy personnel and CEDs in all unit command SOPs, OPLANs, and OPORDs.
 - Incorporating HUMINT collection operations into future plans and operations.
 - Ensuring subordinate units are trained in proper handling and evacuation of captured enemy personnel, materiel, and CEDs.
 - Ensuring that the subordinate elements are trained in OPORDs including ROE and the proper handling of local civilians, foreign nationals, refugees, and DPs.
 - Obtaining, organizing, and supervising employment of additional personnel as guards for EPWs and other detainees where MP assets are not available or insufficient.
 - Tasking the Division/Brigade Engineer Officer in conjunction with the G2/S2 to conduct a site survey for possible EPW/detainee holding area facilities within the operational area. Priority should go to existing facilities needing little or no renovation to meet operational requirements. If suitable facilities cannot be found, the engineer officer should provide detailed facilities design specifications to the G4/S4 for coordination and development of contracted resources.
- G4/S4 responsibilities related to HUMINT collection include but are not limited to—
 - Developing command policy for evacuation and internment of captured enemy personnel, and evacuation and safekeeping of CEE and CEDs.
 - Coordinating contracts for real estate and construction of source-holding facilities if local capabilities are not available. Ideally, existing facilities will be occupied and renovated whenever possible.
 - Collecting and distributing captured enemy supplies. (This is coordinated with the intelligence and operations staffs.)
 - Procuring and distributing rations to personnel holding areas.
 - Transporting EPWs and other detainees in a timely, safe manner to the appropriate facility for processing.

- Determining requirements for use of source labor for the logistical support needed in source-handling operations.
- Providing logistical support to interpreter personnel.

- G5/S5 responsibilities related to HUMINT collection include but are not limited to—
 - Coordinating with local US government, personnel staff representatives, and HN armed forces for procuring native linguists for interpreter support.
 - Coordinating military support of populous.
 - Providing technical advice and assistance in reorientation of sources and enemy defectors.
 - Coordinating MI aspects of CMO activities with the G2.

ADDITIONAL SUPPORT

4-60. In addition to the major staff elements, a HUMINT collection element requires support from several other elements in order to conduct operations. These elements are discussed below.

- The US Army Criminal Investigation Command is the organization with primary responsibility for investigating allegations of criminal acts or reportable incidents committed by or against detainees.
- The SJA can provide legal support and advice on the interpretation and application of applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOS. The SJA is also a channel for reporting known or suspected reportable incidents of abuse or inhumane treatment.
- The Inspector General is a channel for reporting known or suspected reportable incidents of abuse or inhumane treatment.
- The PMO is the channel for reporting criminal activity other than reportable incidents, but also can be used for reporting known or suspected reportable incidents.
- The Chaplain can also receive reports of reportable incidents.
- The G7 provides information on Information Operations and conducts liaison with PSYOP, the Electronic Warfare Officer, the Military Deception Officer, and Operations Security personnel.

This page intentionally left blank.

PART TWO

HUMINT Collection In Military Source Operations

Part Two discusses HUMINT collection as it pertains to MSO. The Secretary of Defense (SECDEF) has established a DOD-wide HUMINT Enterprise consisting of the following executors: The Office of the Secretary of Defense (OSD), the Combatant Commands (COCOMs), the Military Departments, the Defense Intelligence Agency (DIA). All Defense HUMINT Enterprise executors support and satisfy Defense requirements by employing their available resources and capabilities.

MSO refer to the collection of foreign military and military-related intelligence by humans from humans. MSO are conducted under SECDEF authorities, to satisfy DOD needs in compliance with DOD policy. Within the Army, MSO are conducted by trained personnel under the direction of military commanders. These specially trained personnel may employ the entire range of HUMINT collection operations. MSO sources include one-time, continuous, and formal contacts, from contact operations; and sources from interrogations, debriefings, and liaison activities.

Each type of MSO activity has specific operational requirements, specific legal restrictions, and operational guidelines. HUMINT collection activities in each of these categories require specific approval, coordination, and review. MSO include human source contact operations, debriefing, liaison, and interrogations. This chapter introduces each of these collection operations.

Chapter 5

HUMINT Collection

HUMINT COLLECTION OPERATIONS

5-1. Full spectrum operations require focused MSO with strong capabilities dispersed across the battlefield. In offensive and defensive operations, the HCTs need to be placed in support of the engaged maneuver battalions. In stability and reconstruction operations and civil support operations, the HUMINT teams need to be located in battalion AOs throughout the AOIR.

5-2. The rapid pace of operations, the need to provide near-real time (NRT) support of command decisions and the inherent time delays in moving detainees, including EPWs and civilian refugees to centralized locations, necessitate the dispersion of HUMINT collection assets to forward areas in

support of critical operations rather than their retention at detainee and refugee holding facilities at echelons corps and below. This forward deployment gives HUMINT collectors earlier access to sources and is facilitated by enhanced communication and automation capabilities down to the collection team level.

5-3. All operations are different, and deployment of HUMINT assets is METT-TC dependent. Brigades need the capability to provide 24-hour HUMINT collection capability to each battalion AO. The command relationship of the HUMINT collection capability is also METT-TC dependent. The OMT should be located at the echelon that is best able to manage and support the HCTs and to provide the best capability to answer the commander's PIRs.

5-4. The Division and Corps elements should cover their respective areas not covered by their subordinate commands. They also, as needed, reinforce those target areas that are most effective in answering their respective command PIRs already covered by subordinate command capability. EAC HUMINT units normally are responsible for supporting theater or national requirements and providing HUMINT support at theater level facilities such as the JIDC. The EAC units will also augment the echelon below corps units and conduct source operations in the Corps area as required. Operations, particularly in challenging terrain and in stability and reconstruction environments, may require additional HUMINT assets normally obtained from the RC.

HUMAN SOURCE CONTACT OPERATIONS

5-5. HUMINT collection requires the contact between the HUMINT collector, who attempts to gather information through a variety of HUMINT collection techniques, and a human contact, who hopefully has the information that the HUMINT collector wants and who can be convinced to divulge the information. Operations with formal contacts are only conducted by HUMINT collectors and CI agents who are specifically trained and authorized to do so. There are three levels of contacts:

- One-time contact.
- Continuous contact.
- Formal contact.

5-6. The basic goal of all levels of contact is to collect information in response to collection tasking; however, only under certain conditions can HUMINT collectors task contacts to get information for them (see para 5-28). Understanding the types of contacts is key to understanding each type of human source contact operation. The following levels are not all-inclusive nor are the listed categories exclusive. For example, a contact who was initially a one-time contact (such as a walk-in) may later be developed into a continuous contact. A continuous contact may be developed into a formal contact, who can then be tasked, trained, and paid. There is no limit on the number of times a team can meet contacts without recruiting them and making them into a formal contact.

ONE-TIME CONTACT

5-7. The one-time contact is a source of information of value that was, and will be, encountered only once. In all operational environments the HUMINT collector will frequently encounter a source only once, particularly at lower echelons. This may be a local civilian encountered during a patrol, a detainee who is quickly questioned and then evacuated, or a refugee at a checkpoint.

5-8. In addition to the information obtained from a one-time contact, the HUMINT collector must make a reasonable effort to obtain as much basic data as possible about the one-time contact. Complete name, occupation, address, and other basic data of this source are crucial for a thorough analysis of the information provided. The one-time contact and the information he provides cannot be assessed and evaluated independently; however, the information provided by a one-time contact must be reported and corroborated through other HUMINT sources and even other intelligence disciplines.

5-9. Contact reports must be filed with the OMT and source registries maintained in accordance with FM 34-5 (S//NF), AR 381-100 (S//NF), and DIAM 58-11 (S//NF) in order to support analysis of information obtained. If a one-time contact is encountered for a second time and again provides information of value, then the contact may be thereafter treated as a continuous contact.

5-10. A walk-in is a one-time contact who volunteers information of value to US forces on his own initiative. The walk-in source may volunteer information by approaching an HCT, other ISR elements, or US forces or civilian personnel anywhere in the AO. Each unit must have in place a program to identify, safeguard, and direct the walk-in to the appropriate collection asset, to be screened and debriefed as required. For example, a walk-in who wanted to report a crime would be directed to the PMO rather than to a HUMINT collector.

5-11. The collection asset will screen the walk-in to determine the type of information the source has and to determine and evaluate the reliability of the individual. After identifying the type of information, the collector determines if he has the jurisdiction to collect that information. If, for example, the walk-in wishes to report a crime, the collector refers that individual to the proper criminal investigative agency.

5-12. Systematic questioning, deception detection techniques, and cross-checking of information are used extensively in the evaluation process. Concurrently, there are national level directives, DOD directives, and Army regulations that direct specific actions to be taken with a walk-in. When dealing with a walk-in source, HUMINT collectors must guard against adversary intelligence collection. They must also protect legitimate sources of information. The walk-in is thoroughly debriefed on all areas of information relevant to collection requirements, and any information of value is reported.

5-13. On occasion, the HUMINT collector may determine that a one-time contact has the potential to become a continuous contact or a formal contact. This is referred to as a developmental lead. A developmental lead is an

individual identified through social and professional status, leads, source profiling, or other techniques, who has knowledge required by the commander. A developmental lead is any person the HUMINT collector expects to see or would like to see again, or a person who indicates that they intend to return in the future.

5-14. When a HUMINT collector identifies a developmental lead, he reports his interest in elevating the source to continuous or formal contact status as soon as possible to the OMT. Although not every developmental lead becomes a source of information, the HUMINT collector should see each developmental lead as a potential source of information and apply the appropriate security measures. The developmental lead is continuously assessed to verify his placement and access to the type of information the HCT is seeking. Additionally, the HUMINT collector continuously assesses the motivation and characteristics of the developmental lead.

5-15. A one-time source cannot be tasked to collect information, but can be sensitized to information in which the HUMINT collector is interested. For example, if a walk-in source provides information on activity in a house in his neighborhood, he might ask if the collector would be interested in more of the same type information in the future. The HUMINT collector cannot tell him to go get more information, but can indicate that he would listen if the walk-in returned with more information on the topic. If the walk-in returns a second time, he must be handled as a continuous contact.

CONTINUOUS CONTACTS

5-16. Continuous contacts are individuals who have been identified as having more information than could be obtained through a one-time contact, and have been met again by HUMINT collection personnel for the purpose of collecting additional information. HUMINT collectors do **not** task continuous contacts, but they can be sensitized in the same way as one-time contacts. Continuous contacts provide their knowledge through informal debriefings and elicitation.

5-17. All contacts who are seen more than once by HUMINT collectors must be tracked by registering them in the Source Registry and reporting the contacts to the OMT. As an example, a one-time contact who reported information to a HCT contacts them again with follow-up information. That person will now be registered as a continuous contact and tracked by the OMT. This registration process helps to prevent the same information from being collected by multiple collectors from the same contact without realizing it. See AR 381-172 (S//NF) and FM 34-5 (S//NF) for further information on source registration and for the required forms. Types of continuous contacts are discussed below.

Local National and Third-Country National Employees

5-18. Local national and third-country national employees are non-US personnel from either the country in which the US forces are operating or a third country who are either employed by US forces directly or through a contractor to provide logistical support and services. One of the purposes of locally employed personnel screening is to assess these individuals as

potential sources of information. Local national and third-country national employees can be a prolific source of information about local attitudes and events, particularly in a restrictive environment where US contact with the local population is curtailed. Their information can also be significant in a force protection role. The HUMINT collector must register these individuals with the J/G2X. While the HUMINT collector is assessing the local national employee as an intelligence source, CI agents are assessing the same source pool as potential security risks.

5-19. Coordination between HUMINT collectors and CI elements is essential for deconfliction and to avoid duplication of effort. If the HUMINT collector identifies an employee that may be of CI interest, he should immediately notify the appropriate CI unit.

Displaced Personnel and Refugees

5-20. DPs and refugees are excellent sources of information about denied areas and can be used to help identify threat agents and infiltrators. The degree of access HUMINT collectors have to DPs is dependent on the OPORDs, ROE, and SOFAs in effect. HUMINT collectors can work with CA or other programs dealing with DPs or refugees.

5-21. DPs and refugees are normally considered one-time sources but may be incorporated into other long-term collection programs if their degree of knowledge warrants this. In this case, adherence to the restrictions involving source operations is necessary. Those restrictions can be found in AR 380-10, AR 381-100 (S//NF), DIAM 58-11 (S//NF), DIAM 58-12 (S//NF), and other publications as well as existing ROE and SOFAs.

US Forces

5-22. US forces have many opportunities to interact with the local population in the normal course of their duties in operations. This source perhaps is the most under-utilized HUMINT collection resource. Some US forces, such as combat and reconnaissance patrols, are routinely tasked and debriefed by the appropriate level G2/S2. Others, such as medical teams or engineers who have extensive contact with the local population, should also be debriefed.

5-23. Commanders and staff members who serve as liaison with the local population and local government officials can be fruitful sources of information. CA, PSYOP, MP, and other elements also have legitimate reasons to conduct liaison with local authorities and should be debriefed as appropriate. The friendly force debriefing effort can succeed only with command emphasis.

5-24. HUMINT collection elements need to coordinate with local units to identify those individuals who would be most profitable to debrief and to further coordinate with them for time to conduct the debriefing. Although the S2 and S3 can and should task their soldiers to conduct collection tasks during the course of their normal duties, HUMINT collectors must ensure that their friendly force debriefing effort does not interfere with the primary mission accomplishment of the soldiers being debriefed. HCTs should ensure that the necessary staff S2s and S3s are aware of the HUMINT collection

requirements and request that the staffs incorporate these into their respective collection taskings. The results of debriefings by units should also be disseminated to the HCTs for source development, collection targeting, and analysis.

Official Liaison

5-25. Liaison with local military, government, or civilian agency officials provides an opportunity to collect information required by the commander. The HUMINT collector meets with these officials to conduct liaison, coordinate certain operations, collect information, and obtain leads to potential sources of information. Elicitation is the primary technique used with liaison contacts, although in many cases there is a more formal exchange of information. Information obtained by these elements through liaison normally tends to reflect the official positions of their superiors and may not be entirely accurate or complete.

Detainees

5-26. A detainee is any person captured or otherwise detained by an armed force. An EPW is a detainee who meets the criteria of Articles 4 and 5 of the GPW. (See Appendix A.) Detainees may be interrogated. They are frequently excellent sources of information but in many instances the access of the HUMINT collector to the detainees may be curtailed.

5-27. For example, when supporting a counterinsurgency, the supported government may consider all captured insurgents to be criminals and not allow US forces access to them. In these instances, US HUMINT collectors should attempt to sit in during local questioning; they could submit questions or, at a minimum, coordinate to receive the reports from local authority questioning. US HUMINT collectors must remember that regardless of the legal status of the detainees they must be treated in a manner consistent with the Geneva Conventions. (See Appendix A.)

FORMAL CONTACT

5-28. Formal contacts are individuals who have agreed to meet and cooperate with HUMINT collectors for the purpose of providing information. HUMINT collectors who have met with a particular continuous contact three or more times should consider assessing him for use as a formal contact. Formal contacts meet repeatedly with HUMINT collectors, and their operation and tasking must be carried out in accordance with AR 381-172 (S//NF), DIAM 58-11 (S//NF), and DIAM 58-12 (S//NF).

5-29. Formal contacts are generally local nationals or third-country national employees. Knowledge of their meeting with HUMINT collectors is restricted. This can be accomplished by either disguising the fact that the HUMINT collection personnel are indeed HUMINT personnel, or by concealing the purpose of overt meetings with HUMINT personnel. HCTs take extraordinary measures to protect their relationship with these contacts. Depending on METT-TC factors, meetings with formal contacts may range from overt meetings, which are conducted discreetly in order to protect the

relationship between the source and HUMINT collectors, to meetings whereby only the collector and the source know the meeting has occurred. When contact operations are conducted using this methodology, the operation must be coordinated in accordance with the Under Secretary of Defense for Intelligence (USD(I)) policy cited in Appendix J. Specific direction regarding documentation required for recruitment, and the designation of approval authority (usually the J/G2X) for recruitment of a formal contact, will be specified in Appendix 5 (HUMINT) of Annex B (Intelligence) to the governing OPLAN or OPORD.

DEBRIEFING OPERATIONS

5-30. Debriefing operations refer to the systematic questioning of individuals not in the custody of the US, to procure information to answer collection tasks by direct and indirect questioning techniques. The primary categories of sources for debriefings are friendly forces and civilians including refugees, DPs, and local inhabitants.

5-31. Debriefing operations are those operations directed towards collecting information from a segment of the target population using primarily debriefing techniques. These debriefing operations are separate from the G2/S2 debriefing program to debrief personnel returning from missions. Debriefing operations often include the debriefing of personnel who may not usually be debriefed as part of their assigned duties.

5-32. Normally Army debriefing operations will be directly related to collection tasks at the operational and tactical levels. Strategic debriefing of high-level personnel in response to theater and national level requirements is often under the purview of the DIA/DH. Army HUMINT collectors frequently participate in this type of collection, which is under the control, rules, regulations, and operational guidance of DH.

PRINCIPLES AND GUIDELINES

5-33. Debriefing operations are conducted under the guidelines of DIAM 58-11 (S//NF) and DIAM 58-12 (S//NF). They are further subject to applicable execute orders and the specific ROE and classified "umbrella concept" that apply to the specific AO.

OPERATIONAL CONSIDERATIONS AND REQUIREMENTS

5-34. Debriefing requires relatively unconstrained access to the target audience. Debriefing operations are frequently constrained by the umbrella concept, overt operational proposal (OVOP), and OPORDs. Debriefing is a time- and resource-demanding operation that often shows limited immediate results. Since the potential target audience is so large, debriefing operations require careful planning and careful screening and selection of specific targets.

DEBRIEFING OPERATIONS AT THE TACTICAL LEVEL

5-35. Debriefing operations at the tactical level include the debriefing of elements of the local and transient civilian population in support of ongoing tactical operations. This is different from but often supportive of tactical SCOs as described in Chapter 1. Although tactical SCOs use specific identified sources to obtain and report information, tactical debriefing operations use one-time and continuous contacts to answer requirements. Tactical debriefing operations are frequently combined with tactical interrogation operations and may identify potential sources for tactical SCOs.

REFUGEE FACILITY AND CHECKPOINT OPERATIONS

5-36. Refugee facility and checkpoint operations involve placing HCTs at points where US forces expect to encounter large numbers of refugees. Deployment of HUMINT collectors at checkpoints is normally preferred due to their ability to collect and report more timely information. As in the questioning of detainees, the debriefing of refugees should not delay their movement out of the danger area.

5-37. Checkpoint debriefing is normally done in coordination with MP or combat forces that are manning the checkpoint. Debriefing at refugee camps is used to obtain longer term and less immediate information. HUMINT collection units established at refugee camps coordinate their activities with the CA, MP, NGO, or other organizations that has responsibility for operating the refugee camp.

5-38. In internment facilities operated by the MPs, HUMINT collectors coordinate with MPs for access to the detainees and for guard support. In facilities operated by NGOs, HUMINT collectors coordinate with NGOs for permission to speak to the refugees. NGOs are civilian agencies and may decide not to permit HUMINT collectors to have access to refugees.

FRIENDLY FORCE DEBRIEFING

5-39. Every member of the friendly force is a potential source for HUMINT collection. Friendly force personnel frequently have contact with the threat, civilian population, or the environment. Although many individuals report their information in the form of combat information, many do not report the information, do not realize its significance, or do not know how to report key information. Frequently a systematic questioning by a trained HUMINT collector will identify key information that can contribute to the intelligence picture and help an individual recall details. It also helps to place his information into a systematic format for the analyst to use.

5-40. HUMINT collectors debrief selected friendly force personnel including combat patrols, aircraft pilots and crew, long-range surveillance teams, deep insert special forces teams, and other high-risk mission personnel. Often the personnel assigned to a sector of responsibility are the first to notice changes in the attitude of the local populace or differences in the mission environment.

5-41. They are also able to provide indicators concerning the mission environment. HUMINT collectors also conduct debriefings of returned

prisoners of war (POWs), freed hostages, returned US defectors, and soldiers reported as missing in action. These debriefings help to determine enemy methods of operations, enemy intentions, POW handling and interrogations, enemy weaknesses, information concerning other POWs not returned, and battle damage assessment (BDA).

5-42. HUMINT assets lose access to valuable information if they are not regularly coordinating with the following elements:

- **Cavalry Troops, Unit Patrols, and Scouts.** Unit patrols and scouts have a unique view of the battle area that sensors cannot detect. During operations, units and scouts often patrol villages or populated areas that are contentious and therefore of interest. The unit will gain valuable information on the current status of the AO, potentially answering intelligence requirements, through mission reporting and debriefing by their unit S2 or HUMINT collector.
- **Military Police.** HUMINT collection assets work with the MPs who gain area knowledge through their extensive foot patrols and vehicular convoys. MPs also staff checkpoints and traffic control points (TCPs) where they interact with large numbers of the civilian populace and encounter people and situations that often answer intelligence requirements. MP guards at any internment facility are a valuable source of information on the attitude and behavior of detainees. HUMINT collectors should coordinate with the MP detainee facility commander in order to obtain information on detainees obtained through custodial observation and conversations.
- **Civil Affairs.** CA units have daily interaction with the civilian populace including key members of the civilian community such as politicians, technical personnel, and military leadership.
- **Psychological Operations.** PSYOP teams often interview civilians on the battlefield to determine the effectiveness of friendly and threat PSYOP campaigns. PSYOP elements also gather information on political, social, and other PSYOP requirements. PSYOP elements produce and disseminate intelligence products based partially on their interaction with the civilian populace.
- **Special Operations Forces.** The Special Operations Forces (SOF) team often has greater access to humans and areas on a battlefield than any other collection asset. Their observation of and interaction with the local population provides them access to information that often answers collection requirements. The following are examples of these types of collection missions:
 - Special reconnaissance missions into denied territory to satisfy intelligence gaps or to confirm information from another source.
 - Unconventional warfare (UW) missions normally of a long duration. SOF are inserted into hostile territory to conduct sensitive operations that support US tactical and national objectives. During these missions, SOF units often come in contact with the local population and gather information that meets intelligence requirements.
- **Long-Range Surveillance.** Direct observation and reporting on targets such as activities and facilities may provide timely and

accurate intelligence to support a decision or cross-cue other collection capabilities. Long-range surveillance (LRS) is often employed when discreet observation of an activity is necessary over a long period of time or when a collection system that can respond to redirection is necessary.

- **Criminal Intelligence Operations.** CID personnel, in cooperation with MP soldiers, play a key role by linking criminal intelligence to specific groups and events. The criminal intelligence collection effort specifically targets weapons, drugs, organized crime, and identities of smuggling routes. The identification of smuggling routes results in a significant increase in numbers of weapons being confiscated. The timely transfer of criminal intelligence products to tactical units enables a rapid response to serious confrontations, increased confiscation of arms and ammunition, and improved stability in a TF and AO. The Fusion Cell within the ACE develops intelligence products from national, theater, and operational sources. Due to the significant threat that criminal elements pose, CID military agents and CID civilian analysts may be attached to the Fusion Cell to facilitate the police intelligence function.

STRATEGIC DEBRIEFING OPERATIONS

5-43. Strategic debriefing is debriefing activity conducted to collect information or to verify previously collected information in response to national or theater level collection priorities. This avoids surprises of a strategic nature and is used to support long-range strategic planning. Strategic debriefing is conducted in peacetime as well as in wartime. It often fills intelligence gaps on extremely sensitive topics or areas. The sources for strategic debriefing include but are not limited to émigrés, refugees, displaced persons, defectors, and selected US personnel. Strategic debriefing guidance is provided in DIAM 58-11 (S//NF), DIAM 58-12 (S//NF), and DODD 3115.09, "DOD Intelligence, Interrogations, Detainee Debriefings, and Tactical Questioning."

5-44. Strategic debriefing is conducted in a non-hostile, business-like manner. The rapport posture is usually amicable as the source is usually willingly answering national level intelligence needs. Although voluntary sources may not be motivated by a desire for money or other material incentives, it is necessary to ensure that any promised incentives are delivered. The time used in a strategic debriefing can range from days to years. Sources typically have high-level backgrounds in scientific, industrial, political, or military areas.

5-45. Information gathered as strategic intelligence is categorized into eight components. Each of these components can be divided into subcomponents. These components and subcomponents are neither all-encompassing nor mutually exclusive. This approach enhances familiarization with the types of information included in strategic intelligence. An easy way to remember these components is the acronym "**BEST MAPS**":

Biographic Intelligence
Economic Intelligence
Sociological Intelligence
Transportation and Telecommunications Intelligence

Military Geographic Intelligence
Armed Forces Intelligence
Political Intelligence
Science and Technological Intelligence

- **Biographic intelligence** is the study of individuals of actual or potential importance through knowledge of their personalities and backgrounds. For further guidance on collecting and reporting biographic intelligence, see DIAM 58-12 (S//NF). The subcomponents are—
 - Educational and occupational history—civilian and military backgrounds of individuals.
 - Individual accomplishment—notable accomplishments of an individual's professional or private life.
 - Idiosyncrasies and habits—mannerisms and unusual lifestyles.
 - Position, influence, and potential—present and/or future positions of power or influence.
 - Attitudes and hobbies—significant interests that may affect an individual's accessibility.
- **Economic intelligence** studies economic strengths and weaknesses of a country. The subcomponents are—
 - Economic warfare—information on the diplomatic or financial steps a country may take to induce neutral countries to cease trading with its enemies.
 - Economic vulnerabilities—the degree to which a country's military would be hampered by the loss of materials or facilities.
 - Manufacturing—information on processes, facilities, logistics, and raw materials.
 - Source of economic capability—any means a country has to sustain its economy (for example, black market trade, legitimate business or trades, and imports and exports).
- **Sociological intelligence** deals with people, customs, behaviors, and institutions. The subcomponents are—
 - Population—rates of increase, decrease, or migrations.
 - Social characteristics—customs, morals, and values.
 - Manpower—divisions and distribution within the workforce.
 - Welfare—health and education.
 - Public information—information services within the country.
- **Transportation and telecommunications intelligence** studies systems dedicated to and used during military emergencies and peacetime.

- **Military geographic intelligence** studies all geographic factors (physical and cultural) that may affect military operations. Physical geography is concerned with natural or manmade geophysical features. Cultural geography provides demographics information.
- **Armed forces intelligence** is the integrated study of the ground, sea, and air forces of the country. The subcomponents are—
 - Strategy—military alternatives in terms of position, terrain, economics, and politics.
 - Tactics—military deployments and operations doctrine.
 - OB—location, organization, weapons, strengths.
 - Equipment—analysis of all military materiel.
 - Logistics—procurement, storage, and distribution.
 - Training—as carried out at all echelons to support doctrine.
 - Organization—detailed analysis of command structures.
 - Manpower—available resources and their conditioning.
- **Political intelligence** studies all political aspects which may affect military operations. The subcomponents are—
 - Government structure—organization of departments and ministries.
 - National policies—government actions and decisions.
 - Political dynamics—government views and reactions to events.
 - Propaganda—information and disinformation programs.
 - Policy and intelligence services—organization and functions.
 - Subversion—subversive acts sponsored by the government.
- **Science and technological intelligence** studies the country's potential and capability to support objectives through development of new processes, equipment, and weapons systems. The subcomponents are—
 - Weapons and weapon systems.
 - Missile and space programs.
 - Nuclear energy and weapons technology.
 - NBC developments.
 - Basic applied science.
 - Research and development systems.

LIAISON OPERATIONS

5-46. Liaison is conducted to obtain information and assistance, to coordinate or procure material, and to develop views necessary to understand counterparts. Liaison contacts are normally members of the government, military, law enforcement, or other member of the local or coalition infrastructure. The basic tenet of liaison is *quid pro quo*. An exchange of information, services, material, or other assistance is usually a part of the transaction. The nature of this exchange varies widely depending upon the culture, location, and personalities involved.

5-47. Because the nature of liaison tasks varies widely, the general goals of the liaison operation and the objective of each liaison contact should be

clearly defined. The objective should include the type of information to be collected, methods of operations unique to the area, and the command objectives. Additionally, the collector should know limitations on liaison activities. These limitations include—

- Prohibitions against collecting certain types of information or contacting certain types of individuals or organizations.
- Memorandums of understanding with other echelons which delineate each echelon's AOR and AORs for subordinate units.
- Coordination requirements per DCID 5/1 dated 19 December 1984, which are required for selected types of liaison activities.

5-48. Administrative considerations include—

- Type, method, and channels of reporting information obtained from liaison activities.
- Project and contingency fund site numbers to be used.
- Funding and incentive acquisition procedures.
- Limitations on the use of ICFs or incentives.
- Reporting system used.
- Authority under which the specific liaison program is conducted and guidelines for joint and combined operations are set.

5-49. Benefits of liaison include—

- Establishing working relations with various commands, agencies, or governments.
- Arranging for and coordinating joint and combined operations.
- Exchanging operational information and intelligence within legal limits.
- Facilitating access to records and personnel of other agencies not otherwise accessible.
- Acquiring information to satisfy US requirements.
- Accessing a larger pool of information.

INTERROGATION OPERATIONS

5-50. HUMINT interrogation is the systematic process of using approved interrogation approaches to question a captured or detained person to obtain reliable information to satisfy intelligence requirements, consistent with applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. Interrogation is to be conducted by personnel trained and certified to use legal, approved methods of convincing EPWs/detainees to give their cooperation. Interrogation sources are detainees, including EPWs.

5-51. Definitions of EPWs and rules for their treatment are contained in the Geneva Convention Relative to the Treatment of Prisoners of War (GPW). The definition and rules for the treatment of civilians are contained in the

Geneva Conventions Relative to the Protection of Civilian Persons in Time of War (GC). (See Appendix A.) For persons covered by those Conventions, applicable GPW and GC provisions must be adhered to at all times. (Regarding treatment of detained personnel, see also paragraph 5-74.)

5-52. There is an additional protocol to the Geneva Conventions called Protocol I Additional to the Geneva Conventions, 1977, which also contains definitions of who is a civilian and who is an EPW (Articles 50 and 44). The US has not ratified Protocol I nor does it accept the expanded definition of EPWs that it contains. Requirements managers, J/G/S2X personnel, and HUMINT collectors should understand, however, that coalition military personnel with whom they may work may be bound by Protocol I, and those coalition personnel may be required to treat additional personnel as EPWs. Any questions concerning the GPW and Protocol I must be directed to the SJA office for clarification.

5-53. Interrogation operations are specific operations normally conducted at detainee collection facilities directed at the wide-scale collection of information from detainees using interrogation techniques. Although field interrogations are conducted at all echelons and during all operations in which there are detainees, detention facilities where interrogation operations occur are normally located only at theater or JTF level.

5-54. Compliance with laws and regulations, including proper treatment of detainees, is a matter of command responsibility. Commanders have an affirmative duty to ensure their subordinates are not mistreating detainees or their property. HCT leaders must effectively supervise their subordinate collectors during all interrogation operations. Supervisors must ensure that each HUMINT collector has properly completed an interrogation plan and sound collection strategy, and fully understands the intelligence requirements he is seeking to satisfy prior to beginning an interrogation. NCOs and WOs should regularly participate in interrogations with their subordinates to ensure that the highest standards of conduct are maintained. Interrogation supervisors should also monitor interrogations by video, where video monitoring is available. The production, use, and dissemination of interrogation videos must be tightly controlled by HCT leaders. Such videos must not be released for dissemination outside the Intelligence Community without the express permission of the SECDEF or his delegate.

NON-DOD AGENCIES

5-55. Non-DOD agencies may on occasion request permission to conduct interrogations in Army facilities. These requests must be approved by the JTF commander or, if there is no JTF commander, the theater commander or appropriate higher level official. The interrogation activity commander will assign a trained and certified interrogator to escort non-DOD interrogators to observe their interrogation operations. The non-DOD personnel will sign for any detainee they want to question from the MPs, following the same established procedures that DOD personnel must follow. In all instances, interrogations or debriefings conducted by non-DOD agencies will be observed by DOD personnel. In all instances, non-DOD agencies must observe the same standards for the conduct of interrogation operations and

treatment of detainees as do Army personnel. All personnel who observe or become aware of violations of Army interrogation operation standards will report the infractions immediately to the commander. The personnel who become aware of mistreatment of detainees will report the infractions immediately and suspend the access of non-DOD personnel to the facility until the matter has been referred to higher headquarters. Non-DOD personnel conducting interrogation operations in an Army facility must sign a statement acknowledging receipt of these rules, and agree to follow them prior to conducting any interrogation operations. Non-DOD personnel working in DOD interrogation facilities have no authority over Army interrogators. Army interrogators (active duty, civilian, or contractor employees) will only use DOD-approved interrogation approaches and techniques.

FOREIGN GOVERNMENT INTERROGATORS

5-56. Foreign governments may request to participate, or may be invited to participate in interrogations in Army facilities. Requests for foreign government access to detainees will be forwarded through the operational chain of command for appropriate action pursuant to DOD policy. Foreign government personnel must comply with US DOD policies and observe the same standards for the conduct of interrogation operations and treatment of detainees as do Army personnel. The interrogation activity commander will assign a trained and certified interrogator to escort foreign government interrogators to observe their interrogation operations. The foreign government personnel will sign for any detainee they want to question from the MPs, following the same established procedures that US DOD personnel must follow. In all instances, interrogations or debriefings conducted by foreign government interrogators will be observed by US DOD personnel. In all instances, foreign government interrogators must observe the same standards for the conduct of interrogation operations and treatment of detainees as do US Army personnel.

MP FUNCTIONS IN ASSOCIATION WITH INTERROGATION OPERATIONS

5-57. MP and MI personnel both have responsibilities with regard to EPW/detainees, but with different goals and responsibilities. (See DOD Directive 3115.09.) Therefore, close coordination must occur between MP and MI personnel in order to facilitate the effective accomplishment of the MP and MI missions. Both MP and MI personnel must ensure that they treat detainees in accordance with the baseline standards of humane treatment.

5-58. MPs are responsible for the humane treatment, evacuation, custody and control (reception, processing, administration, internment, and safety) of detainees; force protection; and the operation of the internment facility, under the supervision of the provost marshal. The MPs do not conduct intelligence interrogations. Intelligence interrogation is strictly a HUMINT function. DOD policy requires that all detainees in its control, whether or not interrogation has commenced, are assigned an internment serial number as soon as possible, normally within 14 days of capture. (See AR 190-8.)

5-59. The standard MP security and internment functions are the only involvement the MPs have in the interrogation process. MPs will not take any actions to set conditions for interrogations (for example, "softening up" a detainee). For purposes of interrogation, military working dogs will not be used.

5-60. MPs may support interrogators as requested for detainee custody, control, escort, and/or additional security (for example, for combative detainees). When interrogators promise an incentive to a detainee, the interrogators must coordinate with the MPs to ensure that the detainee receives the incentive and is allowed to retain it. MPs may provide incentives in support of interrogation operations under the following conditions:

- Using incentives is coordinated with and approved by the MP facility commander.
- Providing and withdrawing incentives does not affect the baseline standards of humane treatment. This means that MPs can provide incentives such as special food items. However, when the incentive is withdrawn, the MPs still must provide the normal rations.
- Using incentives does not violate detainee custody and control or facility security. This means that if a HUMINT collector requests MPs to provide an incentive (for instance, specialty food) but the detainee has been spitting on the guards, then MPs would not provide the incentive because it might reinforce inappropriate behavior.

5-61. MPs exercise the overall responsibility for the safety of detainees, even in those cases in which detainees are in the temporary custody of HUMINT collectors or other agency personnel for the purpose of interrogation. HUMINT collectors should arrange with the MP supervisor to debrief MP guards. Guards who observe and interact with detainees can report the detainees' disposition, activities, mood, and other observable characteristics.

5-62. HUMINT collectors conduct interrogations for intelligence information. They normally work within the confines of the detainee detention facility, but have no involvement in the mission of the security of detainees. MPs follow a strict protocol concerning access to detainees. Accompanied and unaccompanied access to detainees must be coordinated and approved in advance by the MP commander responsible for the detainees or that commander's designated representative.

5-63. When HUMINT collectors coordinate for a detainee interrogation in an internment facility, the MPs escort the detainee to the interrogation site, which is collocated with, or located within the internment facility. MPs verify that the HUMINT collector is authorized access to the detainee. Depending on security concerns, the HUMINT collector may request that the MP remain, or he may request the MP depart until the detainee needs to be returned to the living area. If the MP remains, his functions are to maintain the security, accountability, and safety of the detainee and the safety of the interrogator, interpreter, and others in the interrogation site. The MP will perform no role in the interrogation. When conducting interrogations in a holding area such as a detainee collection point (DCP), MPs may not be available to provide security for interrogation operations. In that case, the

HUMINT collector will need to arrange for security from the unit that has established the holding area.

5-64. If the MP departs the immediate area where the detainee is being questioned (for example, asked to wait outside the interrogation room), the HUMINT collector will assume custody and responsibility for the detainee by signing for the detainee, noting the detainee's physical condition.

5-65. SOPs should be written to comply with a requirement that interrogation operations will always be under observation, whether conducted in fixed sites, holding areas, or in the field. Physical setup and logistical availability will dictate whether observation is conducted directly, from a concealed location, or by video monitoring. HUMINT collectors should never be alone with a detainee without being under observation.

5-66. Once a HUMINT collector has assumed custody of a detainee, he will not turn the detainee over to anyone other than an MP. Specifically, he will not allow another government agency to assume custody from him. The HUMINT collector will instead return the detainee to the custody of the MP, and the agency seeking custody of the detainee will then be required to do so from the MP. Likewise, HUMINT collectors will not assume custody of a detainee directly from another government agency, but will require them to return the detainee directly to the custody of the MP.

LEGAL, REGULATORY, AND POLICY PRINCIPLES AND GUIDELINES

5-67. The GPW (Appendix A, Section I), the GC (Appendix A, Section III), and the UCMJ are relevant documents pertaining to interrogations of detainees.

5-68. The approaches, psychological techniques, and other principles presented in this manual must be conducted in accordance with applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. US policy is to treat all detainees and conduct all interrogations, wherever they may occur, in a manner consistent with this commitment. Authority for conducting interrogations of personnel detained by military forces rests primarily upon the traditional concept that the commander may use all available resources and lawful means to accomplish the mission and to protect and secure the unit.

"Prisoners of war do not belong to the power for which they have fought; they are all under the safeguard of honor and generosity of the nation that has disarmed them."

—Napoleon, The Military Maxims of Napoleon 1927, ed. Burnod

POINT OF CAPTURE THROUGH EVACUATION

MP Functions	HUMINT Functions
• Maneuver and Mobility Support Operations • Area Security • Internment and Resettlement Operations • Law and Order Operations • Police Intelligence Operations • Ensure detainee abuse is avoided and reported	• Screen and question detainees at TCPs and checkpoints • Question contacts, local civilians, refugees, and EPWs • Conduct liaison with military and civilian agencies • Report information obtained • Ensure detainee abuse is avoided and reported • Support DOCEX

DETENTION FACILITY

MP Functions	HUMINT Functions
• Detain and guard EPWs, civilian internees, and other detainees • Conduct reception and processing • Coordinate Classes I, II, and VIII supplies • Coordinate NGOs, PVOs, and interagency visits • Ensure detainee abuse is avoided and reported • Transport detainees within the detention facility to interrogation area • Maintain security during interrogation operations	• Debrief guards • Screen detainees and EPWs for PIR and IR • Provide linguist support when possible • Observe detainees under MP control • Ensure detainee abuse is avoided and reported • Conduct interrogations • Report information obtained • Cross-cue other intelligence disciplines (as needed) • Support DOCEX

Figure 5-1. MP vs HUMINT Responsibilities.

5-69. The Geneva Conventions establish specific standards for humane care and treatment of enemy personnel captured, retained, or detained by US military forces and its allies. All persons who have knowledge of suspected or alleged violations of the Geneva Conventions are obligated by regulation to report such matters through command channels or to designated individuals, such as the SJA or IG. For example, HUMINT collectors who are working with others must ensure that no incidents of detainee abuse occur, whether committed by a fellow HUMINT collector, an interpreter, HN or coalition personnel, MP, representative of another government agency, or anyone else.

5-70. Failure to report a suspected or alleged violation of the law of war may subject the service member to disciplinary actions. Violations of the Geneva Conventions committed by US personnel may constitute violations of the UCMJ. The commander is responsible for ensuring that the forces under his command comply with the Geneva Conventions. If violations occur in the conduct of warfare, the commander bears primary responsibility for investigating and taking appropriate action with respect to the violators.

5-71. Every soldier has the duty to report serious incidents, whether observed or suspected, in accordance with AR 190-40. Such incidents are reported to the chain of command. If the chain of command itself is

implicated, the soldier can report the incident to the SJA, IG, chaplain, or provost marshal.

5-72. There are reasons for reporting serious incidents beyond those related to legal requirements. For instance, the publishing of enemy war crimes can be used to influence public opinion against the enemy. Also, reporting war crimes of other countries provides important information that may become relevant, since we would not be able to transfer detainees to any power that we could not rely on to treat them appropriately under the law of war, including the Geneva Conventions.

5-73. Several articles of the GPW apply to HUMINT collectors and interrogation operations. Excerpts from some of the most relevant articles of the Geneva Conventions are listed below. Although the following excerpts are specific to EPWs, service members must treat all detainees captured during armed conflict consistent with the provisions of the GPW unless a determination to the contrary is made. Moreover, US policy requires that US forces apply the principles of the Geneva Conventions, during military operations. (See Appendix A.)

- Article 5 - Should any doubt arise as to whether persons having committed a belligerent act and having fallen into the hands of the enemy, belong to any of the categories enumerated in Article 4, such persons shall enjoy the protection of the present Convention until such time as their status has been determined by a competent tribunal.
- Article 13 - PWs must at all times be treated humanely. Any unlawful act or omission by the Detaining Power causing death or seriously endangering the health of a PW in its custody is prohibited. Likewise, PWs must at all times be protected, particularly against acts of violence or intimidation and against insults and public curiosity.
- Article 14 - PWs are entitled, in all circumstances, to respect for their persons and honor. Women shall be treated with all regard due to their sex, and shall in all cases benefit by treatment as favorable as that granted to men.
- Article 15 - The Power detaining PWs shall be bound to provide, free of charge, for their maintenance and medical attention required by their state of health.
- Article 17 - This article covers several requirements with direct impact on interrogation.
 - Every PW, when questioned on the subject, is bound to give only his surname, first names and rank, date of birth, and army, regimental, personal or serial number, or failing this, equivalent information. If he willfully infringes this rule, he may render himself liable to a restriction of the privileges (emphasis added) accorded to his rank or status.
 - For example, this does not mean if a prisoner fails to give this information he loses status as a prisoner, only special privileges. An example might be an officer who fails to identify himself as such. An officer cannot be compelled to work (Article 49). An officer who fails to identify himself as such could lose this privilege.

 - The questioning of PWs shall be carried out in a language they understand.
 - No physical or mental torture or any other form of coercion may be inflicted on EPWs to secure from them information of any kind whatever. PWs who refuse to answer may not be threatened, insulted, or exposed to unpleasant or disadvantageous treatment of any kind.
- Article 18 - All effects and articles of personal use, except arms, horses, military equipment and documents, shall remain in the possession of PWs, likewise their metal helmets and protective masks and like articles issued for personal protection. Effects and articles used for their clothing or feeding shall also remain in their possession, even if such effects and articles belong to their regulation military equipment.
 - Badges of rank and nationality, decorations and articles having above all a personal or sentimental value may not be taken from PWs.
 - Sums of money carried by PWs may not be taken away from them except by order of an officer, and after the amount and particulars of the owner have been recorded in a special register and an itemized receipt has been given, legibly inscribed with the name, rank, and unit of the person issuing said receipt. (Note: Unit SOP should require initial impounding of all sums of money from detainees, properly documented and accounted for, in order to prevent detainees from using money to buy influence of any kind, or participate in black market or other improper activity.)
- Article 19 - PWs shall be evacuated, as soon as possible after their capture, to camps situated in an area far enough from the combat zone for them to be out of danger. Only those PWs, who, owing to wounds and sickness, would run greater risks by being evacuated than by remaining where they are, may be temporarily kept back in a danger zone.
- Article 33 - Medical personnel and chaplains, while retained by the Detaining Power with a view to assisting PWs, shall not be considered as PWs. They shall, however, receive as a minimum, the benefits and protection of the Geneva Convention. They shall continue to exercise their medical and spiritual functions for the benefits of PWs.

5-74. **All captured or detained personnel, regardless of status, shall be treated humanely, and in accordance with the Detainee Treatment Act of 2005 and DOD Directive 2310.1E, "Department of Defense Detainee Program," and no person in the custody or under the control of DOD, regardless of nationality or physical location, shall be subject to torture or cruel, inhuman, or degrading treatment or punishment, in accordance with and as defined in US law.** All intelligence interrogations, debriefings, or tactical questioning to gain intelligence from captured or detained personnel shall be conducted in accordance with applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E,

"The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. Use of torture is not only illegal but also it is a poor technique that yields unreliable results, may damage subsequent collection efforts, and can induce the source to say what he thinks the HUMINT collector wants to hear. Use of torture can also have many possible negative consequences at national and international levels.

Cruel, Inhuman or Degrading Treatment Prohibited

All prisoners and detainees, regardless of status, will be treated humanely. Cruel, inhuman and degrading treatment is prohibited. The Detainee Treatment Act of 2005 defines "cruel, inhuman or degrading treatment" as the cruel unusual, and inhumane treatment or punishment prohibited by the Fifth, Eighth, and Fourteenth Amendments to the U.S. Constitution. This definition refers to an extensive body of law developed by the courts of the United States to determine when, under various circumstances, treatment of individuals would be inconsistent with American constitutional standards related to concepts of dignity, civilization, humanity, decency and fundamental fairness. All DOD procedures for treatment of prisoners and detainees have been reviewed and are consistent with these standards, as well as our obligations under international law as interpreted by the United States.[1]

Questions about applications not resolved in the field by reference to DOD publications, must be forwarded to higher headquarters for legal review and specific approval by the appropriate authority before application.

The following actions will not be approved and cannot be condoned in any circumstances: forcing an individual to perform or simulate sexual acts or to pose in a sexual manner; exposing an individual to outrageously lewd and sexually provocative behavior; intentionally damaging or destroying an individual's religious articles.

[1] Nothing in this enclosure should be understood to affect the U.S. obligations under the law of war.

5-75. **If used in conjunction with intelligence interrogations, prohibited actions include, but are not limited to—**

- Forcing the detainee to be naked, perform sexual acts, or pose in a sexual manner.
- Placing hoods or sacks over the head of a detainee; using duct tape over the eyes.
- Applying beatings, electric shock, burns, or other forms of physical pain.
- "Waterboarding."
- Using military working dogs.
- Inducing hypothermia or heat injury.
- Conducting mock executions.
- Depriving the detainee of necessary food, water, or medical care.

5-76. While using legitimate interrogation techniques, certain applications of approaches and techniques may approach the line between permissible actions and prohibited actions. It may often be difficult to determine where

permissible actions end and prohibited actions begin. In attempting to determine if a contemplated approach or technique should be considered prohibited, and therefore should not be included in an interrogation plan, consider these two tests before submitting the plan for approval:

- If the proposed approach technique were used by the enemy against one of your fellow soldiers, would you believe the soldier had been abused?
- Could your conduct in carrying out the proposed technique violate a law or regulation? Keep in mind that even if you personally would not consider your actions to constitute abuse, the law may be more restrictive.

5-77. If you answer yes to either of these tests, the contemplated action should not be conducted. If the HUMINT collector has any doubt that an interrogation approach contained in an approved interrogation plan is consistent with applicable law, or if he believes that he is being told to use an illegal technique, the HUMINT collector should seek immediate guidance from the chain of command and consult with the SJA to obtain a legal review of the proposed approach or technique. (See paras 5-80 and 5-81 for information on responding to illegal orders.) If the HUMINT collector believes that an interrogation approach or technique is unlawful during the interrogation of a detainee, the HUMINT collector must stop the interrogation immediately and contact the chain of command for additional guidance.

CAUTION: Although no single comprehensive source defines impermissible coercion, certain acts are clearly prohibited. Certain prohibited physical coercion may be obvious, such as physically abusing the subject of the screening or interrogation. Other forms of impermissible coercion may be more subtle, and may include threats to turn the individual over to others to be abused; subjecting the individual to impermissible humiliating or degrading treatment; implying harm to the individual or his property. Other prohibited actions include implying a deprivation of applicable protections guaranteed by law because of a failure to cooperate; threatening to separate parents from their children; or forcing a protected person to guide US forces in a dangerous area. Where there is doubt, you should consult your supervisor or servicing judge advocate.

5-78. Security internees are detainees who are not combatants but who pose a security threat, may be under investigation, or who pose a threat to US forces if released. HUMINT collectors are required to treat all detainees humanely. EPWs are entitled to additional protections guaranteed by the GPW that security internees may not be eligible for. For example, allowing a security internee to communicate with a family member (a right that an EPW has under the Geneva Conventions) could allow him to pass information that would compromise a sensitive investigation and endanger the lives of soldiers and civilians. HUMINT collectors should consult with their SJA for clarification of detainees' status and rights.

5-79. HUMINT collectors are employed below brigade level when the combat situation requires limited tactical interrogation at battalion or lower.

HUMINT collectors should also provide training in the area of tactical questioning to designated S2 personnel. The potential for abuse of the detainee is greatest at initial capture and tactical questioning phase. With the excitement and stress of the battlefield, unskilled personnel may exercise poor judgment or be careless and thus resort to illegal techniques to elicit critical information. Personnel who are not trained HUMINT collectors will not attempt to use approach techniques. Instructions must stress the importance of the proper treatment of detainees. Emphasize that in addition to legal requirements, the abuse of a detainee at the initial stage of contact often renders future interrogation futile. All treatment of detainees must be consistent with the Geneva Conventions. (See ST 2-91.6 for further information on tactical questioning.)

5-80. Orders given to treat detainees in any way that violate the Law of War, including the Geneva Conventions, or that result in detainees being treated in any prohibited manner are unlawful. Every soldier must know how to respond to orders that he perceives to be unlawful. If a soldier receives an order that he knows to be unlawful, or that a person of ordinary sense and understanding would know to be unlawful, or if the order is not clear enough to determine if it is legal or not, he should follow the steps set out below (preferably in the order listed):

- Ask for clarification.
- State that the order is illegal if he knows that it is.
- Use moral arguments against the order.
- State the intent to report the act.
- Ask the senior interrogator to stop the act.
- Report the incident or order if the order is not withdrawn or the act in question is committed.
- If there appears to be no other recourse, refuse to obey the unlawful order.

NOTE: If the order is a lawful order, it should be obeyed. Failure to obey a lawful order is an offense under the UCMJ.

5-81. None of the above actions should be taken in the presence of any detainee. Witnessing actions taken to determine the legality of an order may lead to increased resistance of the detainee and could lead to increased resistance throughout the detainee population if they believe they are being treated unlawfully.

5-82. Illegal orders or incidents must be reported to the chain of command. However, if the chain of command itself is implicated, report the incident or order to the SJA, IG, chaplain, or provost marshal.

OPERATIONAL CONSIDERATIONS AND REQUIREMENTS

EPW Evacuation System

5-83. The MPs are responsible for evacuating detainees, civilian internees, and other detainees, as stipulated in AR 190-8. HUMINT collection assets must be placed to take advantage of the evacuation system the MPs will put into place. The evacuation of detainees and civilian internees normally is a slow and cumbersome process that can severely tax a maneuver unit's resources. Appendix D explains the handling of detainees in detail, including the 5Ss—Search, Silence, Safeguard, Segregate, and Speed to the Rear. The 5Ss are authorized with respect to handling detainees for the purposes of movement of detainees and security. The 5Ss are not authorized for use as interrogation approach techniques.

5-84. The initial evacuation of detainees and civilian internees is the responsibility of the capturing unit. That unit is normally responsible for moving the detainees and civilian internees from the point of capture to the nearest DCP. Under MP doctrine, the MPs are responsible for the detention, security, processing, safety, well-being, accountability, and humane treatment of detainees and civilian internees.

5-85. Normally the MPs assume responsibility for the further evacuation of the detainees and civilian internees; however, under certain circumstances, other units could be charged with this task. The detainees are normally evacuated from a DCP to a short-term collection facility and then finally to a theater internment facility. Once the theater internment facility (joint) is established, dependent on METT-TC factors, the internment facility escort guard units may go forward as far as the initial collection points and escort detainees and civilian internees to a short-term collection facility or straight to a theater internment facility.

5-86. Senior MP commanders coordinate and synchronize transportation and security requirements with MP divisional and BCT leaders. It may take 8 hours for a detainee to reach the DCP; 8 to 16 hours more to reach a short-term collection facility; and 24 additional hours to reach the theater internment facility. Mandatory timelines will be determined in command policy guidance. Critical during this process is that MPs work closely with MI, SJA, and interagency personnel to determine the proper status of individuals detained. Determining whether an individual is an EPW, a criminal insurgent, or in another status is crucial to facilitate the release or transportation, holding, and security requirements. This determination will be used when the individual's biometric data is taken and entered into the Biometric Automated Toolset (BAT).

5-87. The HUMINT collection assets need to be positioned to maximize their collection potential and take advantage of the time available during evacuation. The rapidity of operations and the need to facilitate the commander's situational understanding—coupled with the technological innovations that link the HUMINT collector to databases, analysts, and technical support from anywhere on the battlefield—require placing the HCTs forward into brigade and even maneuver battalion areas to provide

immediate access to EPWs/detainees. EPWs/detainees are normally interrogated for tactical information in the maneuver battalion trains areas and then questioned in detail at the theater JIDC.

Security

5-88. When dealing with detainees, the HUMINT collector faces two security considerations: his own physical security and information security. Particularly when operating in support of tactical operations, the HUMINT collector is in close contact with enemy soldiers who could attempt to escape and may attack the HUMINT collector in doing so. Detainees during a stability and reconstruction operation are often people committed to a cause who find themselves in desperate circumstances. Although the detainees are normally under guard, the HUMINT collector must always be alert to any physical threat posed by these individuals. He must also ensure that his own actions do not provide the detainee with the means with which to harm the collector or anyone else.

5-89. The HUMINT collector should also be aware that EPWs and other detainees may attempt to elicit information. Since HUMINT collectors, by virtue of their position, may possess a great deal of classified information, they must be careful not to reveal it unwittingly in the process of questioning a detainee.

PROHIBITION AGAINST USE OF FORCE

Acts of violence or intimidation, including physical or mental torture, or exposure to inhumane treatment as a means of or aid to interrogation are expressly prohibited. Acts in violation of these prohibitions may be a violation of US law and regulation and the law of war, including the Geneva Conventions of 1949, and may be criminal acts punishable under the UCMJ and other US law. Moreover, information obtained by the use of these prohibited means is of questionable value. If there is doubt as to the legality of a proposed form of interrogation, the advice of the SJA must be sought before using the method in question.

Limitations on the use of methods identified herein as expressly prohibited should not be confused with psychological ploys, verbal trickery, or other nonviolent or non-coercive subterfuge used by the trained HUMINT collector in the successful interrogation of hesitant or uncooperative sources. Use of torture by US personnel would bring discredit upon the US and its armed forces while undermining domestic and international support for the war effort. It also could place US and allied personnel in enemy hands at a greater risk of abuse by their captors. Conversely, knowing the enemy has abused US and allied POWs does not justify using methods of interrogation specifically prohibited by law, treaty, agreement, and policy. In conducting intelligence interrogations, the J2/G2/S2 has primary staff responsibility to ensure that these activities are performed in accordance with these laws and regulations. **[*The commander bears the responsibility to ensure that these activities are performed in accordance with applicable law, regulations, and policy. The unit must have an internal SOP for execution of the interrogation mission.]**

The psychological techniques and principles in this manual should neither be confused with, nor construed to be synonymous with, unauthorized techniques such as brainwashing, physical or mental torture, including drugs that may induce lasting or permanent mental alteration or damage. Physical or mental torture and coercion revolve around eliminating the source's free will, and are expressly prohibited by GWS, Article 13; GPW, Articles 13 and 17; and GC, Articles 31 and 32.

> *Torture is an act committed by a person under the color of law specifically intended to inflict severe physical or mental pain and suffering (other than pain or suffering incidental to lawful sanctions) upon another person within his custody or physical control. (Extracted from Title 18 of the United States Code, Section 2340A).*

*Emphasis added for use in this manual.

Capture Rates

5-90. Anticipating not only overall capture rates but also capture rates linked to specific operations is vital to the correct placement of HUMINT collectors supporting interrogation operations. Defensive and stability and reconstructions operations normally provide a small but steady flow of detainees while successful offensive operations can overwhelm HCTs. To be successful, HUMINT collection support to tactical operations must be carefully planned and prioritized. Available HUMINT collection assets must be balanced against the operations objective, enemy situation estimate, and projected EPW capture rates. The unit S2 is responsible for projecting capture rates.

Interrogating Wounded and Injured Detainees

5-91. Commanders are responsible to ensure that detainees receive adequate health care. Decisions regarding appropriate medical treatment of detainees and the sequence and timing of that treatment are the province of medical personnel. Detainees will be checked periodically in accordance with

command health care directives, guidance, and SOPs, applicable to all detainees to ensure they are fit for interrogations. Detainees determined by medical personnel to be medically unfit to undergo interrogation will not be interrogated. Health care personnel will be on call should a medical emergency arise during interrogation. Health care personnel will report detainees' conditions, as appropriate, to the commander. Health care providers shall not be placed in a position to advise on the application or duration of interrogation approach techniques.

5-92. Wounded and otherwise injured detainees can be a valuable source of information. For evacuation purposes, medical personnel may classify detainees as walking wounded or sick or as non-walking wounded or sick. Walking wounded detainees are evacuated through normal evacuation channels. Non-walking wounded are delivered to the nearest medical aid station and evacuated through medical channels.

5-93. HUMINT collectors may interrogate a wounded or injured detainee provided that they obtain permission from a competent medical authority and that the questioning will not delay or hinder medical treatment. Questioning will not delay the administration of medication to reduce pain or the evacuation of the detainee to where they may receive medical treatment, nor will interrogation be allowed if it would cause a worsening of the condition of the detainee. In most cases, this simply requires the HUMINT collector to ask the doctor, medic, or other medical personnel if it is all right to talk to the detainee.

5-94. With the doctor's permission, the HUMINT collector may talk to the detainee before, after, or during medical treatment. The HUMINT collector cannot at any time represent himself as being a doctor or any other type of medical personnel. Nor can he state, imply, or otherwise give the impression that any type of medical treatment is conditional on the detainee's cooperation in answering questions.

TYPES OF INTERROGATION OPERATIONS

5-95. There are two general categories of interrogation operations: **field interrogation operations** and **interrogation facility operations**.

FIELD INTERROGATION OPERATIONS

5-96. Field interrogation operations constitute the vast majority of interrogation operations at echelons corps and below. Field interrogations include all interrogation operations not conducted at a fixed facility. Current doctrine emphasizes the placement of HCTs forward with maneuver units to provide immediate interrogation support while the information is fresh and the detainee may still be susceptible to approaches, due to the shock of capture. The rationale for this method of employment is twofold:

- First, the pace of the modern battlefield no longer allows the luxury of waiting for a detainee to reach a collection point prior to interrogation. Commanders need more timely information, including HUMINT. Also, automated tools and improved communications now permit rapid transmittal of information from forward-deployed HCTs.

- Second, current MP doctrine has the theater level EPW escort companies picking up detainees as far forward as the division forward collection points and bypassing the intervening collection points.

5-97. An added benefit of placing the HCTs with maneuver units is that it allows them to conduct other HUMINT collection activities, such as the debriefing of local civilians and refugees concurrently with interrogation operations. HCTs are allocated to maneuver units based on—

- The relative importance of that subordinate element's operations to the unit's overall scheme of maneuver.
- The potential for that subordinate element to capture detainees, documents, and materiel or encounter civilians on the battlefield.
- The criticality of information obtained from those sources to the success of the parent unit's overall OPLANs.

5-98. As the mission and situation change, the HCTs are redistributed. As MI assets, they should never be kept in reserve.

5-99. During offensive and defensive operations, HCTs normally operate with maneuver brigades and battalions. HUMINT collectors with battalions or brigades should be equipped with vehicles and communications systems that are compatible with the systems organic to the supported unit. HUMINT collectors with brigades and battalions receive their collection priorities from the S2 of the supported unit. In stability and reconstruction operations, the HCTs normally operate in the AOs of battalion and brigade TFs.

INTERROGATION FACILITY OPERATIONS

5-100. Joint interrogation operations are operations conducted at higher echelons, usually at, and in coordination with, EPW and detainee internment facilities. The Joint Forces Commander (JFC) normally tasks the Army component commander to establish, secure, and maintain the EPW internment facility system. The corps may have the mission of establishing an interrogation facility when it is acting as the Army Forces (ARFOR) or Land Component Command (LCC) element.

5-101. An echelon above corps (EAC) MP brigade normally operates the theater internment facility. The subordinate JFC with a J2 staff lead establishes a Joint Interrogation and Debriefing Center as an activity within the theater internment facility. The MI Brigade Commander or other named SIO is normally designated as the JIDC commander. Army interrogation operations are normally carried out in an area of the MP-operated internment facility set aside for that use.

5-102. The JIDC is normally administratively and operationally self-sufficient. A JIDC will function as part of an overall detainee command and control structure as outlined in FM 3-19.40 and/or by policy. Continuous coordination between the JIDC commander and internment facility commander is essential. The JIDC will—

- Normally consist of facility headquarters, operations, analysis, editorial, interrogation, screening, and DOCEX elements.

- Collocate with the theater detainee internment facility.
- Organizationally structure itself to meet METT-TC requirements within the theater.
- Include HUMINT collectors, CI personnel, technical experts, personnel for CEDs and DOCEX, and intelligence analysts, as applicable, from the Army, Air Force, Marine Corps, Navy, and other government agencies.
- Maintain the capability to deploy HCTs forward, as needed, to conduct interrogations or debriefings of sources of interest who cannot be readily evacuated to the JIDC.
- Often establish a combined interrogation facility with allied HUMINT collector or interrogator augmentation if operating as part of a multinational operation.
- Receive collection guidance from the C/J/G2X and send its intelligence reports to the C/J/G2X and to the supported C/J/G/S2.

5-103. The exact size and organizational structure of these elements will vary dependent on METT-TC.

Headquarters Element

5-104. The activity headquarters provides all command, administrative, logistic, and maintenance support to the JIDC. It coordinates with—

- Higher headquarters for personnel, intelligence, and operational and logistical support prior to and after deployment.
- Theater J2 for reporting procedures, operational situation updates, theater and national level intelligence requirements, and collection priorities.
- Provost marshal for location of theater detainee internment facilities and for procedures to be followed by HUMINT collectors and MPs for the processing, interrogating, and internment of EPWs.
- Commanders of theater medical support units and internment facility for procedures to treat, and clear for questioning, wounded EPWs.
- Commanders of supporting CI and TECHINT assets to establish support requirements and procedures.
- The servicing SJA.
- Magistrate for Article 78 issues.
- Commanders of Air Force, Marine, Navy, and national level organizations to arrange administrative and logistic interoperability.

Operations Element

5-105. The operations element controls the daily activities within the JIDC. The JIDC operations element—

- Ensures that work areas are available for all JIDC elements.
- Establishes and maintains JIDC functional files, logs, and journals.
- Makes detainee files available to detainee release boards to assist the board members in their determinations.
- Establishes interrogation priorities.

- Disseminates incoming and outgoing distribution.
- Conducts coordination with local officials, adjacent and subordinate intelligence activities, CI, MP, PSYOP, the Joint Captured Materiel Exploitation Center (JCMEC), Plans and Policy Directorate (J5), and provost marshal.
- Conducts coordination with holding area officer in charge (OIC) for screening site, medical support, access, movement, and evacuation procedures for detainees.
- Conducts operations briefings when required.
- Supervises all JIDC operations and establishes SOPs.
- Supervises all intelligence collection activities within the JIDC.
- Ensures observers are present when OGAs use the JIDC's interrogation rooms.

Analytical Element

5-106. The analytical element normally is directly subordinate to the operations element. The JIDC analytical element ensures that collection requirements are current and validated. It reviews reports to ensure that the information reported is in response to validated collection requirements. In addition, they ensure an up-to-date common operational picture (COP) by maintaining digital mapping of the current tactical situation and with OB updates to help HUMINT collectors maintain their situational awareness. At locations where digital mapping is not possible, paper situation maps (SITMAPs) are maintained. This element also—

- Obtains, updates, and maintains the database.
- Works with interrogators to provide collection focus for interrogations.
- Establishes and maintains OB workbooks and files including data generated by intelligence information which has not been verified.
- Maintains digital or paper SITMAPs, as available, displaying enemy and friendly situations.
- Catalogs, cross-references, and disseminates collection requirements to JIDC collection elements.
- Reviews interrogation reports for inclusion into the database.
- Conducts situation briefings when required.
- Conducts intelligence reach with the J2 analytical cell and other analytical elements, such as INSCOM Information Dominance Center, for relevant information and analysis.

Editorial Element

5-107. The editorial element is normally directly subordinate to the operations element. It reviews all outgoing reports for format, content, and completeness.

DOCEX Element

5-108. At a minimum, the JIDC will contain a small DOCEX element to translate, screen, and extract information from and report on information of

intelligence interest from source-associated documents. The theater joint document exploitation facility (JDEF) may be collocated with the JIDC. In this instance, the JDEF will translate, screen, categorize, and exploit all types of CEDs.

Screening Element

5-109. The JIDC normally has a separate screening element to receive and screen all incoming detainees and their personal effects. The screening element will review previous screening reports, which should have been sent along with the detainees; recommend priorities for interrogation; identify individuals of interest to other agencies; and may conduct limited interrogations for PIR information. The exact size of the element will vary based on detainee capture rates and detainee flow. Interrogation elements should use their most experienced interrogators as screeners in order to quickly and effectively select the detainees for interrogation who are most likely to possess useful information.

Interrogation Element

5-110. The interrogation element assigns HUMINT collectors to specific detainees, uses interrogation and other HUMINT collection methods to obtain information in response to intelligence requirements, and produces intelligence reports (IIRs and SALUTE reports) as well as source-related operational reports. The interrogation element may also debrief returning US POWs and other personnel as deemed relevant.

This page intentionally left blank.

PART THREE

The HUMINT Collection Process

Part Three discusses the logical progression of phases involved in all HUMINT collection. There are five phases and the related task of screening that are critical to HUMINT collection. This remains consistent with previous doctrine as captured in the interrogation process but adds screening as a phase and combines approach and termination. The five phases are screening, planning and preparation, approach and termination strategies, questioning, and reporting.

Chapter 6

Screening

6-1. Available human sources and documents almost always exceed the qualified HUMINT collection assets and resources that can be applied against them. Screening facilitates the efficient application of these limited assets and resources to maximize the collection of relevant information.

HUMAN SOURCE SCREENING

6-2. As it applies to HUMINT operations, screening is the process of evaluating and selecting human sources and documents for the prioritized collection of information based on the collection requirements and mission of the unit conducting the screening or its higher headquarters. Screening categorizes and prioritizes sources based on the probability of a particular source having priority information and the level of cooperation of the source. Screening is also used to determine if a source matches certain criteria that indicate that the source should be referred to another agency. Screening is conducted at all echelons of command and in all operational environments. There are two general categories of screening: human source screening and document screening. Human source screening will be explained in depth in this chapter. Document screening is explained in Appendix I.

6-3. The resources (time and personnel) allocated to screening must be balanced against those required for interrogations, debriefings, and other collection methodologies. Although screening is not in itself an information collection technique, it is vital to the rapid collection of information. Through screening, the effectiveness of limited collection assets can be maximized by targeting those assets against the sources with the highest potential of providing key information. Screening requires experienced individuals with

maturity and judgment who are totally knowledgeable of the collection requirements and able to make well-reasoned decisions based on limited information. Collection (interrogation, debriefing, and elicitation) can be integrated into screening activities; however, it slows the screening process and decreases the number of potential sources that can be screened.

6-4. Human source screening is the evaluation of an individual or a group of individuals to determine their potential to answer collection requirements or to identify individuals who match a predetermined source profile. The purpose of screening is to—

- Identify those select individuals among the target audience who have information of potential value and who are willing or can be persuaded to cooperate.
- Identify individuals who match certain criteria that indicate them as being potential subjects for source operations or matching the profile for collection by special interest groups such as TECHINT or CI.

6-5. Screening requires the development of criteria that are indicators of potential information. These might include rank, position, gender, ethnic group, appearance, and location.

6-6. Screening is an integral part to all HUMINT collection operations. While questioning an individual source, a HUMINT collector may switch between screening (finding out general source areas of knowledge) to interrogation, debriefing, or elicitation (finding out detailed information about a specific topic). In operations, such as EPW or refugee operations that involve large numbers of potential sources, screening will normally be conducted as a separate but collocated operation as part of the overall interrogation or debriefing effort. The high number of potential sources being dealt with in most human source screening operations requires a systematic approach be developed and utilized to make the most effective use of the personnel and resources being allocated to the source screening operation.

SCREENING OPERATIONS

6-7. Like all intelligence operations, human source screening operations are focused on certain targets. Although the exact target population group will depend on the requirements of the theater of operations, the target focus of source screening operations is best described as the permanent and transitory population in the AO. This definition includes local indigenous populations, refugees, and travelers in the area, and detainees (including EPWs). Specifically excluded from this definition are members of the HN forces (military and paramilitary), members of allied forces, and members of HN government agencies who are available to US forces through liaison operations. Other personnel not indigenous to the AO (such as legitimate NGOs, humanitarian organizations, UN personnel) are available to US forces for voluntary debriefing and should be excluded from screening operations.

6-8. Screening operations may be conducted in a variety of situations and are dependent on the operational situation and the population. Although every source screening operation has the same basic purpose, each can be directed against different segments of the population in different locations throughout

the AO. In order to accommodate the differences in the screening audience and location, different types of source screening operations are employed.

- Tactical Screening. Tactical screening is conducted in support of combat or contingency operations. It can include the screening of EPWs or detainees at the point of capture, the screening of refugees, or the screening of local civilians in cordon and search. At the tactical level, there is no time for elaborate approach techniques so the degree of cooperation becomes a prime concern. Tactical area screening is characterized by rapidly changing requirements, the need to evacuate noncombatants and detainees to a secure area, and the need to collect priority tactical information while operations are in progress. Although the most lucrative type of source is often the detainee, all available sources should be screened for priority tactical information. In tactical screening, the HUMINT collector normally accompanies the maneuver force (OPCON or DS). If the HUMINT collector establishes that the source has information of value during screening, he immediately questions the source. Information collected is passed to the maneuver commander, normally via SALUTE reports. The HUMINT collector may recommend to the commander that individual sources be further detained for additional questioning. Screening must be done accurately in order that a commander can make a decision to detain or release possibly hostile personnel, based on the recommendation of a HUMINT collector.
- Checkpoint Screening. Checkpoints are often established to screen the local populations as they transit through and within the AO or to screen large numbers of individuals such as refugees or DPs as they enter the AO. Screening checkpoints can be static or mobile. HUMINT collectors must pay particular attention to refugees leaving the area ahead of friendly forces (AO or AOI). It is likely that refugees can provide information of tactical value more quickly and easily than detainees. Refugees know the area and may be able to identify for the collector anything that is out of the ordinary, such as insurgent or terrorist activities.
- Local Population Screening. This refers to the screening of the local population within their own neighborhoods. When HUMINT collectors move into a new area, they must observe the local population and determine who may be able and willing to provide the information they have been tasked to collect. Once this determination is made, the collectors must engage those individuals in conversation to assess their level of knowledge.
- Collection Facility Screening. Screening is conducted as a normal part of HUMINT collection operations at collection facilities such as theater interrogation and debriefing facilities and refugee camps. Screening is coordinated with the unit, normally an MP unit that is responsible for the operation of the facility.
- Local Employee Screening. CI personnel periodically screen local employees to determine possible security risks. Concurrently, local employee screening may identify sources who can provide information to answer the CCIRs. Close coordination between HUMINT and CI collection assets is a must in local employee screening.

- Variations and Combinations. All types of screening can be adapted to meet specific circumstances slightly different from those for which they were designed. Additionally, it is possible to use more than one type of screening in an operation if the specific circumstances require it.

6-9. Screening of refugees, EPWs, and other detainees normally occurs at two locations: initially at the point where friendly forces first encounter them and again when they arrive at the theater and other holding areas or refugee camps. The capturing or detaining forces should enforce segregation of EPWs from refugees and other detained civilians; they should be screened in separate operations, one screening for EPWs and one for refugees and other detained civilians. Depending on METT-TC factors, segregation should be conducted as follows:

- Refugees: Refugees, even if of the same nationality as the enemy, are not treated as enemies exclusively based on their nationality and are not automatically subject to control measures. If refugees are encountered on the battlefield, they are segregated from EPWs and screened separately. They are generally not detained further unless some additional reason requires their detention. At a refugee camp, screening will be done in coordination with the NGO operating the refugee camp. If there is a reason to detain refugees for further questioning for intelligence purposes, or because they pose a security threat, they will then be treated as a detainee. Under all circumstances, refugees will be treated humanely. If they are transported to an internment facility, they will be in-processed by MPs and their Geneva Conventions status will be determined. Their status under the Geneva Conventions will afford them certain privileges.
- EPWs: Officers are segregated from enlisted. The enlisted are divided into NCOs and lower enlisted. Males are segregated from females. This segregation facilitates rapid screening for EPWs who may have information to answer PIRs and IRs as well as prohibits officers from influencing enlisted personnel to resist questioning.
- Other Detainees: Civilians should be screened separately from EPWs. As with refugees, if there is a reason to detain civilians for further questioning for intelligence purposes, or because they pose a security threat, they will then be treated as a detainee. Whether or not civilian detainees are released or detained further, screeners should ensure that the civilian detainees are treated humanely. If the civilian detainees are transported to an internment facility, they will be in-processed by MPs and their Geneva Conventions status will be determined. Once detainees are in-processed into an internment facility, they are then considered to be civilian internees and their status as such will afford them certain privileges under the Geneva Conventions.

SCREENING AT FORWARD LOCATIONS

6-10. The initial screening and subsequent questioning should be accomplished as far forward as is operationally expedient. If a HUMINT collector is not available, the unit S2 must ensure initial screening and questioning of sources are completed by qualified personnel. At this level, the individual (military or civilian) is questioned for job, unit (if applicable),

mission, PIR and IR, and supporting information (JUMPS). If time allows, the HUMINT collector may collect additional information, such as the source's name, to start a formal source file to preclude duplication at higher echelons. S2s and personnel other than HUMINT collectors should not attempt an approach at this stage.

6-11. HUMINT collectors will only use approach techniques as time and circumstance allow. The prime requirement is to identify the individuals with information of immediate tactical value, to collect that information expediently, and to evacuate the source. In this case, tactical questioning is normally integrated seamlessly into the screening process. This initial screening can also be used to identify individuals for immediate evacuation to a higher echelon facility for detailed questioning. Any screening reports or information reports generated at this level must accompany the EPWs or detainees as they are evacuated. Typically, battlefield screening reports, such as the screening sheet shown in Figure 6-1, will be done on paper in order to allow multiple screeners to work simultaneously. If automation support is available for each screener, an electronic version of the screening report is used, or the "KB Easy" (Figure 10-2), which allows the screener to easily put screening information into a DIA report format and transmit it electronically. (See Chapter 10 for a KB-EZ worksheet.)

6-12. US forces capturing enemy forces or detaining civilians on the battlefield search each individual for weapons, documents, or other material of intelligence interest. Each individual receives a Capture Tag which records basic biographic data such as name, rank, serial number, unit of assignment (military), location of capture, and any special circumstances concerning the capture. (See Appendices E and F.) Each document or item removed from the captive is also "bagged and tagged" to identify from whom it was taken. This initial step is vital, as properly processing captives and their equipment greatly simplifies the screening process. All documents associated with the source and any possessions taken from him must be evacuated with the source, but not on his person. This is to ensure that the next echelon of screeners and interrogators will have the ability to exploit these items for intelligence value, or to support determination of approach strategies.

SCREENING AT REFUGEE CAMPS OR DETENTION FACILITIES

6-13. When a detainee or refugee arrives at an internment facility, refugee camp, or similar facility, a more extensive screening is conducted. The screening sheet is used to facilitate this process. This screening is normally done in conjunction with in-processing into the facility. During in-processing, the MP will assign an Internment Serial Number (ISN) that is registered with the Theater Detainee Reporting Center (TDRC). The ISN will be used to track the detainee throughout the MP detention system. The ISN should not be used in intelligence channels; however, HUMINT collectors should record the ISN on the screening sheet to aid in locating the detainee again. For intelligence reporting purposes, HUMINT collectors will assign the detainee a source reporting number that will be used to identify the detainee and information associated with him, regardless of whether or not the detainee is transported to another facility. The J2 issues source reporting numbers to HUMINT collectors through the OMT.

MP ISN NUMBER:			EVACUATION DATE:
PERSONAL	LNAME(P): _____ LNAME(M): _____ FNAME: _____ MNAME: _____ SVC/ID NO: _____ DOB: _____ LANGUAGES: _____ MARITAL STATUS: M S W D	CAPTURE DATA	DATE: _____ TIME: _____ PLACE: _____ CAP UNIT: _____ CIRCUMSTANCES: _____ _____ DOCUMENTS: _____ _____ WPNS/EQUIP: _____ _____
***	STATUS: M = Military C = Civilian P = Paramilitary ? = Other		
MILITARY	BRANCH: AF AR CG MC NY ___ RANK: _____ FULL UNIT DSG: _____ _____ DUTY PPSN: _____ JOB: _____ STATION: _____ SKILLS: _____ EXPERIENCE: _____	ASSESSMENT DATA	PHYSICAL CONDITION: SEX: M F WOUNDED: Y N _____ REMARKS: _____ _____ MENTAL CONDITION: EDUCATION = _____YRS INTELLIGENCE: AVG+ AVG AVG- MENTAL STATE: _____ _____
CIVILIAN	JOB: _____ ORG: _____ DUTIES: _____ _____ SKILLS: _____ _____		SCREENER: _____ DATE: _____ TIME: _____ COOPERATION: 1(High) 2 3(Low) KNOWLEDGE: A(High) B C(Low) BGW LIST: Y N BGW CODE: ____ SOURCE CATEGORY: A B C D APPROACH: _____
SPECIAL HANDLING REQUIREMENT CODES: _____ _____			
PIR & IR	_____ _____ _____ _____ _____ _____ _____	REMARKS	_____ _____ _____ _____ _____ _____ _____

SAMPLE

Figure 6-1. Screening Sheet.

6-14. When a detainee is in-processed into an internment facility, MPs will assign the detainee's status as an EPW, retained person, protected person, or other status under the Geneva Conventions. Figure 6-2 provides excerpts from FMI 3-19.40 on MP internment and resettlement operations. In an international conflict, individuals entitled to POW status (EPWs) include—

- Members of the regular armed forces.
- Other militias or volunteer corps, and organized resistance movements of a State Party to a conflict, provided they meet each of the following criteria:
 - Commanded by a person responsible for his subordinates.
 - Having a fixed distinctive sign recognizable at a distance.
 - Carrying arms openly.
 - Conducting operations in accordance with the law of war.
- Civilians who accompany the force.
- Crew members of the merchant marine and crews of civilian aircraft of a State Party to the conflict, who do not benefit by more favorable treatment under any other provisions of international law.

6-15. There are other categories specified in Article 4, GPW. Questions with respect to an individual's entitlement to EPW status should be directed to your SJA.

6-16. Retained personnel (see Articles 24 and 26, GWS):

- Official medical personnel of the armed forces exclusively engaged in the search for, or the collection, transport or treatment of wounded or sick, or in the prevention of disease, and staff exclusively engaged in the administration of medical units and facilities.
- Chaplains attached to the armed forces.
- Staff of National Red Cross Societies and that of other Volunteer Aid Societies, duly recognized and authorized by their governments to assist Medical Service personnel of their own armed forces, provided they are exclusively engaged in the search for, or the collection, transport or treatment of wounded or sick, or in the prevention of disease, and provided that the staff of such societies are subject to military laws and regulations.

6-17. Protected persons include civilians entitled to protection under the GC, including those we retain in the course of a conflict, no matter what the reason. A "civilian internee" is a person detained or interned in the United States or in occupied territory for security reasons, or for protection, or because they have committed an offense against the detaining power, and who is entitled to "protected person" status under the GC.

6-18. The term "detainee" may also refer to enemy combatants. In general, an enemy combatant is a person engaged in hostilities against the United States or its coalition partners during an armed conflict. The term "enemy combatant" includes both "lawful enemy combatants" and "unlawful enemy combatants."

- **Lawful enemy combatants:** Lawful enemy combatants, who are entitled to protections under the Geneva Conventions, include members of the regular armed forces of a State Party to the conflict;

militia, volunteer corps, and organized resistance movements belonging to a State Party to the conflict, which are under responsible command, wear a fixed distinctive sign recognizable at a distance, carry their arms openly, and abide by the laws of war; and, members of regular armed forces who profess allegiance to a government or an authority not recognized by the detaining power.

- **Unlawful enemy combatants:** Unlawful enemy combatants are persons not entitled to combatant immunity, who engage in acts against the United States or its coalition partners in violation of the laws and customs of war during armed conflict. For purposes of the war on terrorism, the term "unlawful enemy combatant" is defined to include, but is not limited to, an individual who is or was part of supporting Taliban or al Qaida forces, or associated forces that are engaged in hostilities against the United States or its coalition partners.

Excerpts from FMI 3-19.40, Military Police Internment/Resettlement Operations

ACTIVITIES

The MPs assist MI screeners by identifying captives who may have answers that support PIR and IR. Because MPs are in constant contact with captives, they see how certain captives respond to orders and see the types of requests they make. The MPs ensure that searches requested by MI personnel are conducted out of sight of other captives and that guards conduct same-gender searches.

The MI screeners examine captured documents, equipment and, in some cases, personal papers (journals, diaries, and letters from home). They are looking for information that identifies a captive and his organization, mission, and personal background (family, knowledge, and experience). Knowledge of a captive's physical and emotional status or other information helps screeners determine his willingness to cooperate.

LOCATION

Consider the following when planning an MI screening site:

- The site is located where screeners can observe captives as they are segregated and processed. It is shielded from the direct view of captives and is far enough away that captives cannot overhear screeners' conversations.
- The site has an operation, administrative, and interrogation area. The interrogation area accommodates an interrogator, a captive, a guard, and an interpreter as well as furniture. Lights are available for night operations.
- Procedures are implemented to verify that sick and wounded captives have been treated and released by authorized medical personnel.
- Guards are available and procedures are implemented for escorting captives to the interrogation site.
- Procedures are published to inform screeners who will be moved and when they will be moved.
- Accountability procedures are implemented and required forms are available.

Figure 6-2. MP Support to Screening.

6-19. It may not be immediately evident in a particular theater of operation whether an individual is an unlawful enemy combatant or is associated with or supporting the unlawful enemy combatants of the United States. Consult your J/G/S2 and servicing SJA for information relevant to your theater of operations.

6-20. All captured or detained personnel, regardless of status, shall be treated humanely, and in accordance with the Detainee Treatment Act of 2005 and DOD Directive 2310.1E, "Department of Defense Detainee Program", and no person in the custody or under the control of DOD, regardless of nationality or physical location, shall be subject to torture or cruel, inhuman, or degrading treatment or punishment, in accordance with and as defined in US law. (See Appendix A, GPW Articles 3, 4, 5, 13, and 14.)

6-21. The rights of EPWs are stated in the GPW. They include the right to quarters, rations, clothing, hygiene and medical attention, property, and other rights. EPWs may not renounce their rights to renounce EPW status. (See Appendix A, GPW Article 7, Section I.)

6-22. Retained personnel must receive at least the same benefits as EPWs. They may only be required to perform religious or medical duties, and they may only be retained as long as required for the health and spiritual needs of the EPWs. Retained persons must be returned to their home country when no longer needed.

6-23. Protected persons' rights include protection from physical or moral coercion and from being taken hostage. Protected persons are protected from murder, torture, corporal punishment, mutilation, medical experimentation, and any form of brutality. Protected persons rights are limited, though. They do not have the right to leave captivity and are not immune from prosecution. Protected persons can be screened and identified for intelligence purposes.

SCREENING PROCESS

6-24. At the internment facility, the screening process normally is distinct from the questioning (interrogation or debriefing) process. Dependent on the criticality of the information identified, the source may be questioned immediately for relevant information but will more likely be identified for future questioning. The screening is a more formal process in which the screener attempts to obtain basic biographic data, areas of general knowledge, source cooperation, and vulnerability to select approach techniques in addition to identifying knowledge of critical intelligence tasks. Once the screener has established the basics (source identification, cooperation, and knowledge), he normally passes the source on to the personnel that conduct the questioning. The screener will complete a screening report that will be forwarded in accordance with unit SOPs (see Chapter 10). If a detainee's knowledge is of Joint Forces interest, a knowledgeability brief (KB) should be written and submitted electronically. (A short form KB worksheet is shown at Figure 10-2.) Complete guidance on KBs is contained in DIAM 58-12 (S//NF).

6-25. If the source freely discusses information of PIR value, the screener normally exploits the information fully and completes a SALUTE report. (See Appendices H and I.) If the source's knowledge of PIR information is extensive and he is freely giving the information, the senior screener and the OIC or noncommissioned officer in charge (NCOIC) of the interrogation or debriefing element are notified immediately. They decide if the screener should continue questioning the source or if the source should be handed off to another HUMINT collector. If source-associated documents contain PIR information, the collector will exploit them as fully as possible and write a SALUTE report. (See Appendix H.)

6-26. The source normally is assigned a standard screening code. The screening code is an alphanumeric designation that reflects the level of cooperation expected from the source and the level of knowledgeability the source may possess. Table 6-1 shows the codes for assessing sources. Those sources assigned to the same category are interrogated in any order deemed appropriate by the interrogation or debriefing element.

Table 6-1. Source Screening Codes.

CODE	COOPERATION LEVEL
1	Responds to direct questions.
2	Responds hesitantly to questioning.
3	Does not respond to questioning.
	KNOWLEDGEABILITY LEVEL
A	Very likely to possess PIR information.
B	Might have IR information.
C	Does not appear to have pertinent information.

6-27. Figure 6-3 shows the order in which detainees in the assessed screening categories should be interrogated. Category 1-A sources normally should be the first priority to be questioned. Category 1-B and 2-A would be Priority II. Category 1-C, 2-B and 3-A would be next as Priority III sources, with 2-C, and 3-B being in the fourth group to be interrogated. Category 3-C sources are normally not questioned. This order ensures the highest probability of obtaining the greatest amount of relevant information within the available time. Screening codes may change with the echelon. The higher the echelon, the more time is available to conduct an approach. Appendix B discusses the reliability ratings of information obtained.

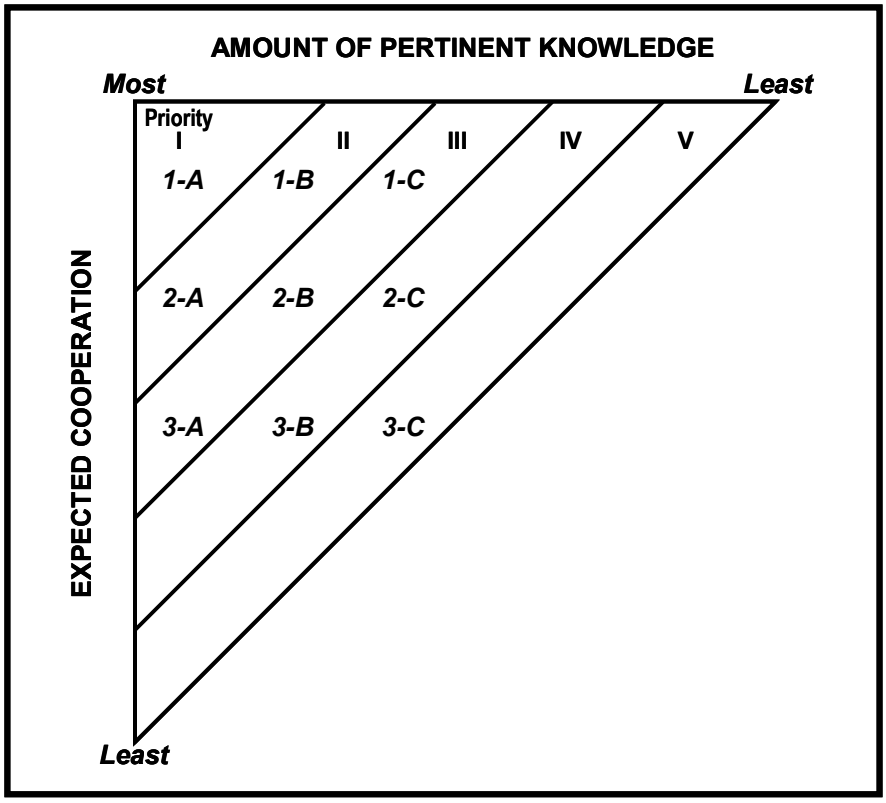


Figure 6-3. Interrogation Priorities by Screening Category.

SCREENING METHODOLOGIES

6-28. Depending on the specific operation or echelon, screening may be a separate operation or may be integrated into a specific collection mission. For example, a HUMINT collector accompanying a patrol encounters a civilian who may have information that is relevant to collection requirements. The HUMINT collector screens the source (that is, asks some general questions to determine the source's level of cooperation and knowledge). Upon receiving a positive response, the HUMINT collector may debrief the civilian on a specific topic or question him on areas of PIR interest. He then reverts to the screening role to determine other relevant knowledge. If the HUMINT collector determines through screening that the source either has no relevant information or cannot be persuaded to cooperate within an operationally expedient timeframe, he is not debriefed as part of the screening process. In detainee or refugee operations, a separate element will normally conduct all screenings. They establish a prioritized list of sources who are then systematically questioned on specific topics by other HUMINT collectors or other technical specialists.

SCREENING REQUIREMENTS

6-29. In addition to potential sources, screening requires several components.

- Collection Requirements. Without a clear list of specific collection requirements, screening becomes virtually impossible. The concept behind screening is to rapidly identify source knowledgeability as it relates to requirements. Screeners should obtain a copy of the supported element's collection requirements and become familiar with the intelligence indicators listed therein. Screeners must use their experience and imagination to devise ways to identify EPWs and detainees who might possess information pertinent to these indicators. Vague requirements (such as "What is the threat doing?") do not provide the focus necessary to make a source selection. The HUMINT collection element must break these SIRs into indicators if the supported intelligence officer has not already done this. The indicators must take into account the type of sources anticipated. For example, a refugee probably will not know if the threat intends to defend a particular ridgeline. However, he might know whether or not there are threat forces on the ridge, if an improvised explosive device (IED) is being employed on a route, if they are digging in, or if engineer type equipment is in the area.
- Selection Criteria. After reviewing the collection requirements, the HUMINT collection element will develop preliminary criteria to identify the source type that will most likely have the required information. The source type may include gender, appearance, military rank, age, or occupation. Some of these criteria are determined by visual observation, thereby saving time in not having to question everyone. Other criteria such as occupation or place of residence may require brief questions.
- Trained Screeners. Screening is possibly the most difficult HUMINT skill. A HUMINT collector must use his experience, questioning skill, cultural knowledge, and knowledge of human nature to decide in a matter of minutes or possibly seconds whether limited HUMINT collection assets and valuable time should be spent talking to an individual based on the way he looks and the answers to a few questions. A wrong decision will mean wasted assets and valuable information missed.
- Language Capability and Cultural Awareness. Screening involves more than asking a series of questions. The HUMINT collector must be able to evaluate the answers, the specific language used, and other clues such as body language to determine the value of an individual to the collection effort. This requires a mature and experienced screener. If the HUMINT collector does not possess the target language, he and his interpreter must be able to work together quickly with mutual trust and confidence.
- Area Conducive to Screening Operations. Effective screening operations must allow the HUMINT collector to speak to the source where the source is not exposed to outside influences or dangers that may inhibit his responses. For that reason, sources should never be screened within the sight or hearing of other potential sources.

HUMINT collectors can use rooms within a building, tents, or other field-expedient methods to isolate the individual being screened. Screening a source within view or hearing of other potential sources may not only pose a danger to the source but also will tend to inhibit the source from freely cooperating.

- Security. The personnel conducting the screening need to be able to concentrate on the individual being screened. Although the collector is ultimately responsible for his own personal security, screening is facilitated by having dedicated personnel present (for example, MPs) who are responsible for security. Screeners coordinate with MP or other security personnel concerning their role in the screening process.

INITIAL DATA AND OBSERVATIONS

6-30. Screening is a filtering process whereby, under ideal circumstances, all potential sources would be questioned to determine if they have information of intelligence interest. In actuality this is often impossible. Screeners often use visual and other aids to "prescreen" the sources in order to eliminate a substantial portion of the target population before conducting detailed screening. For example, if the HUMINT collector at a checkpoint is only interested in information concerning a specific denied geographic area, screeners may ask all refugees if they are from or have been in that denied area recently. A less experienced screener could do this allowing the experienced screener to conduct more extensive screening of the select target audience.

6-31. If time and circumstances permit, screeners should question any friendly personnel who have had extensive contact with the persons to be screened. In the case of detainees, this could include holding area personnel or personnel from the capturing unit. These personnel may be able to help identify sources that might answer the collection requirements or who might match a particular source profile.

6-32. Normally the screener will not have time to conduct any extended observation of the person to be screened; however, the screener should make a quick visual observation of the source prior to questioning him. He should note anything in the source's appearance and behavior that indicates he is willing to cooperate immediately or is unlikely to cooperate. The screener should also note any physical indicators that the source may have the type of information or belong to a certain source profile category.

6-33. Physical indicators include overall appearance such as rank, insignia, and condition of the uniform and type and condition of equipment for military sources and general type and condition of dress (for example, business suit as opposed to work clothes) for civilians. Certain physical indicators (dress, medals such as religious medals, physical type) may be indicators that the source belongs to a specific ethnic or religious group. The source's physical reactions may also indicate a willingness or lack of willingness to cooperate. For example, does the source move forward in the group or attempt to hide within the group; does he intentionally place himself in the wrong segregation group; or does he show any overt signs of nervousness, anxiety, or fright?

6-34. The screeners will also examine all documents and possessions found on the source (if any) and all documents pertaining to the source (if any). **At a minimum, a detainee should have a properly filled out capture tag, which will indicate to the screener where the detainee was captured, by which unit, and under what circumstance.** (See para 6-12 and Appendix D.) Documents such as personal letters, orders, rosters, signal operating instructions (SOIs) and map sections can provide information that identify the source, his organization, mission, and other personal background information (family, knowledge, experience, education). They may in themselves provide information, may identify a source for questioning, and may provide information helpful in assessing a source's susceptibility to an approach.

6-35. Documents pertaining to the source, beginning at the point of capture throughout the evacuation process, such as previous screening and intelligence reports and administrative documents (such as source personnel records prepared by the MPs) help the screener by providing information concerning the source's physical status, emotional status, level of knowledge, level of experience, and other background data. Making timely use of reports from lower echelons can be difficult for the screener, especially when dealing with large numbers of potential sources.

SOURCE ASSESSMENT

6-36. Screeners use standard reporting formats to identify the results of their screening (see Chapter 10). The determination must be made as to whether the source is of any intelligence value to the HUMINT collector. The HUMINT collector will basically place the source within one of four categories.

- Of Immediate Intelligence Interest. This category includes personnel who are assessed, based upon the screening process, who possess information in response to requirements. They are interrogated or debriefed (dependent on their status) to retrieve relevant information. This questioning may be conducted by the same person conducting the screening or by another HUMINT collector.
- Of Interest to Other Agencies. In most cases, the HUMINT collector will be provided with collection requirements by other agencies or disciplines such as TECHINT or CI. In this case the HUMINT collector will question the source on these requirements and report the information appropriately. However, in some instances, particularly in the case of CI, the HUMINT collector may be given a list of topics or a profile of personnel who are of interest to CI. The HUMINT collector will notify the local CI representative when a person matching the "CI profile" is identified. After the HUMINT collector has extracted any relevant intelligence information, he will "pass" the individual off to the CI agents. In many cases, particularly with individuals of TECHINT or other specialized interest, the HUMINT collector will be asked to conduct the questioning with the technical support of the individual from the interested agency. This is coordinated through the HUMINT collector's OMT and the chain of command.

- Of Potential Interest as a Contact Source. On occasion, especially during stability and reconstruction operations, the HUMINT collector may identify an individual who has the potential to provide information in the future, due to his placement or access. Although the individual may not have information of immediate interest, the HUMINT collector will pass his recommendation to the appropriate office, normally the C/J/G/S2X, provided that source operations are authorized (see Chapter 5).
- Of No Interest. This category includes sources who prove (based upon the screening process) to be of no interest to the HUMINT collector or other agencies. Their biographic data is recorded, but they are not questioned further. This category will likely include the bulk of individuals screened. Individuals who have been screened are kept separated from those who have not yet been screened.

OTHER TYPES OF SCREENING OPERATIONS

LOCAL EMPLOYEE SCREENING

6-37. CI personnel conduct local employee screening, primarily to identify individuals who may be a security risk. HUMINT collectors also can use local employee screening as a means to obtain intelligence information or to identify personnel with placement and access to answer information requirements. Employee screening must be conducted in a secure environment and out of the hearing and sight of other employees. Formal written reports of the screening must be maintained.

LOCAL COMMUNITY OR AREA SCREENING

6-38. Local area screening is normally done in coordination with other operations such as a cordon and search operation. The HUMINT collectors accompany the forces conducting the operation and screen the general population to identify individuals of intelligence or CI interest.

SCREENING FOR CI REQUIREMENTS

6-39. Before initiating the screening process, the HUMINT collector establishes liaison with supporting CI agents. The CI element provides CI requirements and provides a profile of personnel of CI interest. CI is normally interested in personnel who—

- Have no identification documents.
- Have excessive or modified identification documents.
- Possess unexplainable large amounts of cash or valuables.
- Are illegal border-crossers.
- Attempt to avoid checkpoints.
- Are on the CI personalities list, which includes members of an intelligence service.
- Request to see CI personnel.
- Have family in the denied area.
- Speak a different language or dialect than is spoken in the area.

6-40. Personnel of CI interest include two general categories of people: The first type of "person of interest" is any individual or group involved in adversary intelligence collection operations or who is attempting to enter the AO to conduct such operations. Examples of these individuals include but are not limited to—

- Known or suspected members and/or supporters of foreign intelligence and security services and known or suspected members and/or supporters of the intelligence activities of non-state entities such as organized crime, terrorist groups, and drug traffickers.
- Known or suspected hostile espionage agents, saboteurs, subversives, or hostile political figures.
- Known or suspected enemy collaborators and sympathizers who may pose a security threat to US forces.
- Personnel known to have engaged in intelligence, CI, security, police, or political indoctrination activities.
- Known or suspected officials of enemy governments whose presence poses a security threat to US forces.
- Political leaders known or suspected to be hostile to the military and political objectives of the US or an allied nation.

6-41. The second type of "person of CI interest" is any individual who possesses information concerning the identification, location, or activities of personnel in the first category.

SCREENING FOR OTHER TECHNICAL COLLECTION REQUIREMENTS

6-42. Other technical areas such as TECHINT, SIGINT, IMINT, MASINT, or other services need to supply the HUMINT collectors with a profile of the individuals with whom they wish to speak. The HUMINT collectors upon identifying such an individual will contact the requesting agency after extracting PIR information.

Chapter 7

Planning and Preparation

7-1. Planning and preparation is one of the five phases of HUMINT collection. HUMINT collection, regardless of the methodology employed, must be a systematic, carefully prepared enterprise. The HUMINT collector engages in general preparation throughout his career. He focuses that preparation to a specific area of the world, specific mission, and specific collection requirements as those become available. Finally, the HUMINT collector focuses his planning and preparation on a specific collection effort with a specific source.

COLLECTION OBJECTIVES

7-2. Each HUMINT collection mission is conducted for a definite purpose. The HUMINT collector must keep this purpose firmly in mind as he proceeds to obtain usable information to satisfy the requirements, and thus contributes to the success of the unit's mission. The HUMINT collector must use the objective as a basis for planning and conducting questioning. The HUMINT collector should not concentrate on the objective to the extent he overlooks or fails to recognize and exploit other valuable information extracted from the source. For example, during HUMINT collection, the HUMINT collector learns of the presence of a heretofore unknown, highly destructive weapon. Although this information may not be in line with his specific objective, the HUMINT collector must develop this important lead to obtain all possible information concerning this weapon.

RESEARCH

7-3. The key to good HUMINT collection is preparation on the part of the collector. The HUMINT collector must understand the environment and particularly its human component, the mission of the supported unit, that unit’s intelligence requirements, his source, and the cultural environment. The ultimate success of a questioning session is often decided before the HUMINT collector even meets the source.

GENERAL RESEARCH

7-4. Due to the quickly changing world circumstances, it is impossible to conduct all the specific research required immediately prior to questioning a source. General research should be completed before entering an AO and continues until operation completion. Areas of research include but are not limited to—

- OPLANs and OPORDs. The HUMINT collector must be familiar with the unit OPLAN and that of its higher headquarters. By thoroughly understanding the unit OPLAN and OPORD, the HUMINT collector

and HUMINT commanders and leaders can anticipate collection requirements, develop source profiles, recommend deployment strategies, and otherwise integrate HUMINT operations into the overall unit operation. Although the OPORD needs to be read and understood in its entirety, certain areas are of critical importance to the HUMINT collection effort. They include—

- Task organization. This will show where HUMINT C2, staff support, and collection assets will fit into the organizational structure.
- Situation. This gives the friendly and enemy situation.
- Mission. This gives the HUMINT collectors insight into how their operations will integrate into the parent unit's operation.
- Execution. The four execution subparagraphs explain the commander's intent on how the mission is to be carried out:
 - Subparagraph 3a (Concept of Operation) includes how subordinate units' operations will be included in the overall plan.
 - Subparagraph 3a(3) (Reconnaissance and Surveillance) details how HUMINT collection operations will integrate into the overall ISR plan. Additional information on ISR is found in Annex L.
 - Subparagraph 3a(4) (Intelligence), along with Annex A (Task Organization) and Annex B (Intelligence), explains how the Intelligence BOS will support the scheme of maneuver.
 - Subparagraph 3d (Coordinating Instructions) lists the CCIRs and initial PIRs.

- Current events. The HUMINT collector must be knowledgeable about current events in all potential operational areas, especially those events that indicate the populace's feelings or intentions toward the US. This will facilitate a better understanding of the cultural, political, and socio-economic conditions that could influence the attitude and behavior of a source. This knowledge can be obtained and updated through classified periodic intelligence publications and/or military or civilian open sources, including both print and broadcast media, CA and PSYOP databases, and the J/G/S2 analytical elements.
- SOPs. The HUMINT collector must be familiar not only with his own unit's SOP but also with that of any supported unit. The HUMINT collector will be able to obtain specific information about report numbers and formats, as well as information about distribution channels for reports from these SOPs. The SOP will also explain unit policy on source exploitation and evacuation procedures, logistic and maintenance functions, and other C2 and support issues.
- Umbrella concept. The TF commander through the J/G2 and J/G2X issues an umbrella concept for HUMINT operations. When operating under this concept, collection parameters will be established in writing, and it is imperative that the HUMINT collector understands his role. Types of sources will be outlined concerning placement, motivation, and access. The umbrella concept will also specify the types of information against which the HUMINT collector can collect. The umbrella concept is governed by AR 381-100 (S//NF), AR 381-172 (S//NF), DIAM 58-11 (S//NF), and DIAM 58-12 (S//NF).

- Legal guides, SOFAs, operations and execute orders, ROE, and other legal and administrative requirements. The HUMINT collector must be thoroughly familiar with all documents that may set the legal parameters for his collection operations. These are available through the chain of command and from the SJA office. He must know how these requirements apply and to what type of sources each is applied.
- Collection requirements. The HUMINT collector needs not only to know but also to understand the requirements that he will be attempting to answer. These requirements can include CCIRs (PIRs and IRs), essential elements of friendly information (EEFIs), Intelligence Priorities for Strategic Planning (IPSP), specific requests from national level consumers such as HUMINT collection requirements (HCRs), SDRs, or even vocal orders given by the local commander. These all will determine the objective of the questioning plan.
- Databases. Intelligence databases can give the HUMINT collector detailed information about the source's unit, its organization, and its capabilities. They also have information on personalities. The HUMINT collector will use information obtained from databases to control the source and assess his answers for truthfulness. They will also give the HUMINT collector ideas of other areas to research. For example, if the threat is primarily a lightly armed insurgent force, studying similar organizations will provide the HUMINT collector with valuable insights into the possible methods of operation of the current target organization.
- SITMAP and COP. The current situation, both friendly and enemy, is vital for the movement of the HCT and for its collection operations. It reflects enemy unit identification, disposition, and boundaries; major roads or trails for movement of personnel, equipment, weapons; and locations of artillery, minefields, roadblocks, entrenchments, obstacles, staging areas, NBC contaminated areas, and ground surveillance devices. All of this information can be used in source questioning as control questions or in otherwise determining source veracity. The HUMINT collector will be able to identify indicators and predict what should be PIRs and IRs.
- INTSUM. The INTSUM provides a summary of the intelligence situation covering a specific period as dictated by the commander. It is already analyzed intelligence.
- Intelligence estimate. The intelligence estimate is derived from the intelligence preparation of the battlefield (IPB). It is based on all available intelligence and considers everything of operational significance. It will help point out gaps in the intelligence database. It is from these gaps that requirements are derived. It will provide information on the mission, AO, weather, terrain, enemy situation, enemy capabilities, and conclusions. It will cover all of the standard OB topics.
- Weapons and equipment guides. Weapons and equipment guides can assist the HUMINT collector in becoming familiar with the type of equipment employed in the AO. Guides are available in hardcopy and softcopy.

- Area handbooks. These handbooks provide detailed information about a specific area of the world. They provide information on political, economic, sociological, cultural, military, biographic, transportation, and geographic topics. The CIA and other agencies publish area handbooks annually. The US Department of State website also has continuously updated information on trouble spots around the world.
- Previous HUMINT reporting. The HUMINT collector should familiarize himself with all previous relevant reporting from the AO. This will provide him with insight into current operations, the types of information collected, and may help identify information gaps.
- Photographs, maps, and other geospatial products. In conducting general research, the HUMINT collector should become familiar with the AOs. This not only will help identify specific areas of HUMINT collection potential but also will be invaluable in both the questioning of specific sources and the maneuver of the HCT.
- Subject matter experts (SMEs) and technical research. Before deploying to an AO or before supporting on a particular mission, the HUMINT collector may identify particular areas in which he lacks critical knowledge. For example, a HUMINT collector who has previously been operating in an area with a conventional enemy may be deployed to an area with an unconventional threat from irregular forces. Also, intelligence requirements may focus on equipment that is unfamiliar to the HUMINT collector. In order to prepare himself, the HUMINT collector contacts SMEs or analysts or uses technical materials to gain background information.
- Other reports. Intelligence agencies publish numerous reports and summaries that are readily available to the HUMINT collector.

CLOSED AND OPEN-SOURCE INFORMATION (USE OF REACH)

7-5. Reach is a process by which deployed military forces rapidly access information from, receive support from, and conduct collaboration and information sharing with other units and organizations (deployed in theater and from outside the theater) unconstrained by geographic proximity, echelon, or command. Intelligence support is established based on requirements that will help the commanders (regardless of echelon) make decisions. Reach can be accomplished in various ways. There is no requirement for all intelligence functional areas or echelons to use the same approach; hence, there is no common standard for all units to use. Each organization or section should develop its strategy on using the various intelligence reach components. Standard enabling tools will provide for easier access than ever before (for example, access to the INSCOM Information Dominance Center).

INTELLIGENCE REACH COMPONENTS

7-6. Intelligence reach requires the G2/S2 to develop a strategy on how best to support the unit's mission with intelligence reach capabilities. There are eight basic elements of the strategy:

- Push: Push occurs when the producers of intelligence or information are knowledgeable of the customer's requirements and are able to send the desired intelligence to the customer without further requests. Push is accomplished through the Joint Dissemination System (JDS) and/or the Automated Message Handling System (AMHS).
- Pull: Pull occurs when the customer is familiar enough with existing databases to be able to anticipate the location of the desired information. Pull is greatly enhanced through the use of portals and homepages with hyperlinks to the various categories of information available to the user. This requires the establishment of such a homepage at each echelon, thus enabling higher echelons to research and pull from lower databases and homepages.
- Database Access: Access to local, theater, DOD, non-DOD, and commercial databases allows analysts to leverage stored knowledge on topics ranging from basic demographics to OB information. A validated DIA Customer Number (acquired by the J2/G2/S2) in combination with SIPRNET and Joint Worldwide Intelligence Communications System (JWICS) connectivity establishes access to most of the databases online.
- Integrated Broadcast Services (IBS): IBS is an integrated, interactive dissemination system, focusing on tactical user's information requirements using a common message Data Element Dictionary (DED) and J-series family of message formats. The goal of IBS is to resolve the uncoordinated proliferation of "stovepiped" intelligence or information broadcasts by providing the tactical commander with integrated time-sensitive tactical information.
- Collaborative Tools: Collaborative tools are computer-based tools (groupware) that help individuals work together and share information. They allow for virtual on-line meetings and data sharing. As much as possible, collaborative tools should be emplaced with all necessary echelons and centers prior to deployment.
- Request for Information: Reach includes the ability of an intelligence officer at any level to request information that is beyond what is available at his location, using the Community On-Line Intelligence System for End Users and Managers (COLISEUM) System. Once an RFI is entered into the system every other user of that system can see it. Hence, an echelon several echelons above the actual requester can and often does become aware of the request and may, in fact, answer it. Reach is also provided through INSCOM's Information Dominance Center and other nodes at J2 and G2.
- Leveraging Collection Management: The collection and ISR management system is established to provide a mechanism for tasking and managing collection assets for required information. Analysts who are trained and familiar with the system and the various tasking procedures can leverage the system for refined information.

- Distributed Common Ground System-Army (DCGS-A): DCGS-A is the ISR fusion and processing system for the future, as part of the overarching DOD-directed DCGS-A surface system family of systems. It will bring national and joint ISR capabilities down to JTF level, corps and division levels and BCT level to provide leaders with NRT information and visualization of threat, weather, and terrain information and intelligence. DCGS-A consolidates the capabilities of the following current-force ground processing systems:
 - All-Source Analysis System (ASAS).
 - Counterintelligence and Human Intelligence (CI/HUMINT) Single-Source Workstation.
 - Tactical Exploitation System (TES).
 - Guardrail Information Node (GRIFN).
 - Guardrail Common Sensor (GRCS) Intelligence Processing Facility (IPF).
 - Prophet Control.
 - Joint STARS Common Ground Sensor (CGS).

7-7. For more information on Intelligence Reach, see FM 2-33.5/ST.

SOURCE-SPECIFIC RESEARCH

7-8. Source-specific research is done immediately prior to questioning the source. The HUMINT collector may have to respond spontaneously in the case of a walk-in source in tactical operations, or if the HUMINT collector has advanced warning as in the case of a planned meeting with a source, a long-term debriefing, or an invitational source. Areas of research include but are not limited to—

- Screening Reports, KBs, Other Reports: Reports about the source not only can provide specific information about the type of information the source can provide to answer specific collection requirements but also can give the HUMINT collector extensive background information about the source. This background information can give clues to information the source might possess and to possible approach techniques. Information contained in screening reports and KBs may provide insight into—
 - Geographic Area: This area may show information about the source's ethnic background, political affiliation, religion, and customs. Information can be obtained from databases, locally registered vital statistics, and residence registries.
 - Languages: Determining the languages and dialects spoken, written, and understood by a source can provide valuable insights into that source's geographic and ethnic or tribal background, education, and social status. This determination of languages and dialects can be facilitated by the use of "flash cards" specific to the battlefield.
 - Other Reports: This can include other reports collected from this source at other echelons or reports from other sources from the same unit or location as the source. It can also include reports or documents published by the ACE at your request.

 - Political Group: This area can provide information on the source's beliefs as well as provide information on political leaders and goals. Additionally, political affiliation can sometimes provide information about subversive groups and paramilitary ties. Knowing the goals of the political organization can also assist the HUMINT collector in choosing an approach or establishing rapport.
 - Religious Affiliation: The source's religious affiliation may provide insight into his motivation, moral strengths and weaknesses, and other motivational factors.
 - Technical Field: Having knowledge about the source's technical field can assist the HUMINT collector in deciding upon which questions to ask. It will also assist the HUMINT collector in verifying the source's truthfulness because the HUMINT collector will have an understanding of the source's specialty.
 - Employment: By researching the source's employment history, the HUMINT collector can discover other areas of information that the source may be able to provide.
 - Education: The source's education level and educational history can not only give the HUMINT collector insight into the possible information the source can provide but also provide insight into possible approach strategies.
 - Social Status: Knowledge of the source's social status may provide a clue to a good approach strategy because the source may be accustomed to a certain type of treatment. It may also provide a clue to biographical information that the source may be able to provide.
 - Criminal Records: Criminal records may also indicate possible approach strategies. Additionally, they may indicate which groups or organizations the source may have knowledge about.
- Documents and Other Media Captured on or in Immediate Association with a Detainee or Brought in by a Debriefing Source: Documents captured with or otherwise pertaining to the source may give the HUMINT collector information about the source, his unit, or his role within that unit. They may answer requirements or indicate knowledge of PIRs. Personal letters, for example, could be used during the approach phase. If a source comes in voluntarily and provides documents, they should be reviewed prior to debriefing the source.
- Photographs, Maps, and Other Geospatial Products: Maps and photographs of the area about which the source is being questioned can give the HUMINT collector an idea of where the source has been and in what kind of terrain he operated, which might indicate knowledge or use of certain tactics. If the HUMINT collector is not familiar with the area the source was in, the HUMINT collector should take some time to look over the map so he can more readily relate when the source mentions locations or dispositions. Aerial photographs show more detailed up-to-date information than maps. They will not normally be as readily available as maps. Maps and other geospatial products will also be needed for use in the map-tracking portion of an interrogation. The HUMINT collector should work with the ACE of the supported unit to obtain them for the AO.

- SMEs: There will be occasions when the HUMINT collector will talk to sources about subjects of which the HUMINT collector has no knowledge. In that case, the HUMINT collector will want to talk to personnel who are SMEs. Depending on the depth of knowledge that the source is expected to have and the time available to prepare, the HUMINT collector may arrange for a technical expert to support the questioning (see Chapter 9).
- Technical Manuals: There are various weapon and equipment identification guides available in hardcopy, softcopy, and off the Internet that can assist the HUMINT collector in identifying any equipment mentioned by the source.
- Source Physical and Mental Condition: HUMINT collectors should observe the source prior to questioning if possible and also talk to anyone available who has relevant information concerning the source. MP guards can be an especially valuable source of information based on source observation and should be debriefed periodically. This can prevent surprises at the onset of the questioning session and can help the HUMINT collector assess the source's physical and mental condition as well as provide insights to possible approaches.
- Databases: Collectors should review source information and reports contained in the various databases available to them. The CHATS system, BAT database, and other databases can provide collectors with source information and previous reporting.

HUMINT COLLECTION PLAN

7-9. After conducting appropriate research, the HUMINT collector working with an analyst, if available, develops a source-based collection plan. This is geared to the specific source that is going to be questioned. The amount of time spent in preparing this plan depends on the operational circumstances. This may range from a quick mental review by an experienced HUMINT collector in a tactical environment to a formal written plan submitted by a subordinate to a team leader. The source collection plan will vary from source to source. It will also vary with the conditions under which the source is questioned. It serves as a checklist to ensure that all steps necessary to prepare for questioning are conducted. Whether written or oral, the HUMINT collection plan should contain at least the following items:

- HUMINT collection requirements.
- Serial number of EPW/detainee to be questioned.
- Location and time for the questioning.
- Primary and alternate approaches.
- Questioning plan including topics to be covered and the planned sequence of these topics.
- Prepared questions for unfamiliar or highly technical topics.
- Method of recording and reporting information obtained.

OBJECTIVE

7-10. The HUMINT collector will first determine the objective of his questioning. The objective is the set of collection requirements that the HUMINT collector will attempt to satisfy during the questioning session. A number of circumstances including the intelligence requirements, the time available, and the source will set the objective. Determining the objective consists of three parts:

- Identify the intelligence requirements. The primary objective of any questioning session is to answer or confirm PIR or other collection requirements.
- Identify the subject: The HUMINT collector will want to consider the source; for example, who he is, what he may know. The HUMINT collector will also want to consider the legal and other restrictions based on the type of source (contact source, EPW, refugee, strategic). For a military source (EPW) this includes rank, position specialty, and unit of assignment. For a civilian source it includes job, placement and access, associations, area of residence, and employment.
- Identify the intelligence requirements that the source may be able to answer. The HUMINT collector cannot normally waste time "fishing" for information. He must determine based on screening, what collection requirements the source can answer. The HUMINT collector compares the information that he gathered through his general and source-specific research and compares it to his list of collection requirements. He compares that list to the identity of the source and refines the list including all requirements that the source can be expected to be able to answer. The HUMINT collector will approach those areas first while staying aware of leads into other collection topics.

LOCATION

7-11. In most cases, the location for the questioning will be determined by operational requirements. However, the HUMINT collector should ensure some basic requirements are met:

- Each questioning session should be conducted outside the hearing and view of third parties. Even in the case of a source meeting in a public place, the HUMINT collector should choose a location where they cannot be overheard and where their meeting will not arouse suspicion.
- The location should be in a place that has reasonable security for the HUMINT collector and the source. In contact operations, the risk cannot always be eliminated but the acceptable risk levels should be based on the expected intelligence gain. In combat operations, most questioning (interrogation, debriefing of civilians on the battlefield) will take place in forward combat areas, but it cannot be done if it increases the risk to the source. Safe evacuation of the sources has priority over questioning.
- The location should provide ready access to the chosen method of recording and reporting the information.

7-12. When conducting military source operations, the location of the questioning will have psychological effects on the source. The questioning location should be chosen and set up to correspond to the effect that the HUMINT collector wants to project and his planned approach techniques. For example, meeting in a social type situation such as a restaurant may place the source at ease. Meeting in an apartment projects informality while meeting in an office projects more formality. Meeting at the source's home normally places him at a psychological advantage, while meeting in the HUMINT collector's work area gives the collector a psychological edge. The HUMINT collector should consider the status and level of the source, security, the workspace available, furnishings, the amount of lighting provided, and the ability to heat or cool the room as needed.

TIME

7-13. Time to conduct questioning should be estimated based on the source, the type of information that the HUMINT collector expects to get, and the complexity of that information. Other considerations include expected evacuation times for sources in tactical situations, the number of other sources that need to be spoken to; and in contact operations, the estimated time that the HUMINT collector can meet with the source without increasing the risk.

7-14. The HUMINT collector must also consider the physical conditions of the source and himself. After extended operations, there may be a limit on how long either the HUMINT collector or source can concentrate on a given subject. Even if the HUMINT collector has an unlimited time period (such as at a joint interrogation and debriefing facility), he must break his questioning down into topical sessions to maximize effectiveness. Time is only an estimate and should be modified based on the circumstances. It may be extended, for example, if the source has a greater than expected amount of information, or critical information in unforeseen areas. The time may be curtailed if the HUMINT collector has met his requirements, the source does not possess the expected information, or a more valuable source is identified.

PRIMARY AND ALTERNATE APPROACHES

7-15. In most circumstances, if the HUMINT collector is meeting with the source for the first time, he should select at least two alternate approaches to use if the direct approach is unsuccessful (see Chapter 8). These approaches need to be based on the HUMINT collector's source-specific research, his general area research, knowledge of the current situation, and knowledge of human nature. There are four primary factors that must be considered when selecting tentative approaches:

- The source's mental and physical state. Is the source injured, angry, crying, arrogant, cocky, or frightened?
- The source's background. What is the source's age and level of military or civilian experience? Consider cultural, ethnic, and religious factors.
- The objective of the HUMINT collection. How valuable is the source's potential information? Is it beneficial to spend more effort convincing this source to talk?

- The HUMINT collector himself. What abilities does he have that can be brought into play? What weaknesses does he have that may interfere with the HUMINT collection? Are there social or ethnic barriers to communication? Can his personality adapt to the personality of the source?

7-16. If the HUMINT collector has a screening sheet or KB, he can use it to help select his approaches. After reviewing the information, the HUMINT collector will analyze the information for indicators of psychological and/or physical weakness that would make a source susceptible to a specific approach. The HUMINT collector also needs to consider his particular strengths and weaknesses in conducting specific approaches. He must consider what immediate incentives he may possibly need and ensure that they are available. Also, if incentives had been previously offered or promised, the collector needs to know if they were in fact provided. If the HUMINT collector has previously questioned the source, he must evaluate the approaches he used and decide if they need to be modified or if additional approach techniques will be needed (see Chapter 8.)

ADDITIONAL SUPPORT REQUIRED

7-17. The HUMINT collector must decide if he will need technical support to include interpreter support.

- Technical support. The HUMINT collector must decide if he will need additional support including analytical, technical, or interpreter support.
- Analytical or technical support. The HUMINT collector must decide if he has the analytical or technical capability to question a specific source. If not, he must decide what degree of support from advice to participation is required of the analyst or technical expert. Any request for analytical or technical support must be coordinated with the 2X. On rare occasions, it may be desirable for the HUMINT collector to seek polygraph support or support from a Behavioral Science Consultant (BSC). BSCs are authorized to make psychological assessments of the character, personality, social interactions, and other behavioral characteristics of interrogation subjects and advise HUMINT collectors of their assessments, as needed.
- Interpreter support. If the HUMINT collector does not speak the needed language or does not speak the needed language well enough to conduct questioning, an interpreter will be required. If the HUMINT collector will need an interpreter, the HUMINT collector will also have to consider the clearance needed to complete the questioning and the availability of the interpreter, as well as the extra time necessary to complete the questioning session. The HUMINT collector will also have to brief the interpreter on the method of interpretation and the HUMINT exploitation plan. Also, he should determine whether there are any cultural aspects associated with the interpreter that may enhance or detract from the success of the meet. (See Chapter 11 for detailed information on HUMINT collection using an interpreter.)

DEVELOP A QUESTIONING PLAN

7-18. The HUMINT collector must develop a plan that will guide his questioning of the source. This includes general topics to be exploited and the sequence in which they will be covered.

7-19. There are two general sequences used in questioning: topical and chronological.

- Topical questioning is used when time is a prime concern, when the source is believed to possess key information in a limited area, when the questioning is concerning a technical topic, or when the source has been talked to previously and this is a subsequent questioning to expand on earlier topics.
- Chronological questioning normally is used when the HUMINT collector is uncertain of the areas of source knowledge, when time is not a factor in questioning, during initial questioning when the source is believed to have knowledge on a large number of topics, and in friendly force mission debriefing.

7-20. A topical sequence is an outline of topics to be questioned in a selected sequence and is based on intelligence requirements or HCRs, as well as a specific source's potential to provide information pertinent to those requirements. The plan serves as a checklist for the HUMINT collector to ensure that all subjects pertinent to the collection objective are questioned in an efficient and organized manner. The HUMINT collector uses his estimate of the type and extent of knowledge possessed by the source to modify the basic topical sequence of questioning. He selects only those topics in which he believes the source has pertinent knowledge. In this way, the HUMINT collector refines his element's overall objective into a set of specific HUMINT collection subjects. In OB factors questioning in either a tactical or strategic setting, and across the full spectrum of operations, the topics covered include missions and the nine major OB factors:

- Composition.
- Strength.
- Dispositions.
- Tactics.
- Training.
- Combat effectiveness.
- Logistics.
- Electronic technical data.
- Miscellaneous.

7-21. See Appendix G for questioning quick reference examples of topics covered under the nine OB factors.

7-22. In strategic and operational debriefing operations the relevant HCR or SDR will guide the HUMINT collector. Regardless of which tasking document is referenced, the topical sequence is established by collection requirements, modified or sequenced, based on source knowledge and time.

7-23. The nine OB factors are not the only guideline that may be used by the HUMINT collector. If the collection objective is something other than a

military unit, many of the OB factors will not fit the collection plan. A helpful memory aid, in this case, is mission, identification, location, and organization (MILO). MILO gives a short, easily remembered structure for questioning nonmilitary or strategic topics. The MILO factors can be questioned in any order, but often the most logical sequence of MILO questioning is identification, organization, location, and mission. Many of the nine OB factors can also fit into the MILO format.

IDENTIFY MEANS OF RECORDING AND REPORTING

7-24. The HUMINT collector will want to decide upon a means of recording the information obtained through source questioning. If the HUMINT collector is planning to use a sound or video recorder, he will also have to consider the availability of the equipment and its positioning (see Chapter 9). Along with the method of recording the information, the HUMINT collector will have to decide on the means of reporting the information (see Chapter 10). Tapes of interrogations must be safeguarded in accordance with DOD Regulation 5200.1-R.

FINAL PREPARATIONS

7-25. After the source-specific questioning plan is developed, the HUMINT collector takes some final preparatory steps.

- Review plan. The HUMINT collector should always go over his collection plan with his supervisor. This review can be written or oral. In addition to the obvious requirements to keep the chain of command informed, this review helps identify any weaknesses in the plan and is a means to effect required coordination and support.
- Collect questioning support materials. The HUMINT collector will want to collect the various references and other guides that he will use to support his questioning. These materials may include source documents, maps, aerial photographs, imagery, OB data, extra lights, extra tables, drawing templates, graph paper, questioning guides, technical reference manuals, city plans and handbooks, and recording devices.
- Conduct required coordination. The HUMINT collector coordinates any support requirements including analytical, technical, or interpreter support, questioning location, ICFs, recording equipment, security, and transportation.
- Organize. The HUMINT collector organizes his materials in a logical manner that will complement his topical sequence. By being organized, the HUMINT collector will not waste time trying to locate the correct manual or guide. Additionally, the HUMINT collector will present a professional appearance to his source.
- Reconnoiter the questioning location. If the questioning location is to be somewhere other than the HUMINT collector's normal AO, such as a public restaurant, the HUMINT collector should conduct an unobtrusive reconnaissance of the site. If at all possible, this should be at the same time and day of the week as the planned meeting. This allows the HUMINT collector to assess the possible security problems

of the location, judge the traffic flow, and identify any other items that might affect the questioning. He can also judge where within the meeting site he can set up for maximum security and psychological advantage. He must be careful that in doing so he does not set up patterns of operation that will increase rather than decrease security problems.

- Set up questioning site. If the HUMINT collector has control over the site where the collection is being conducted, the last step in preparing is the actual setup of the questioning site. The HUMINT collector will want to decide on the placement of the furniture and lighting and where everyone will be seated and decide where he will place his technical support materials.
- Question guards. If the person to be questioned is a detainee, the HUMINT collector should arrange to question MP guards who have been in contact with the detainee to ascertain source behavior, attitude, and other useful information that guards may be able to provide.
- Check with medical personnel. If the detainee was injured or ill, ensure that he was treated by medical authorities and released for questioning.

7-26. The supervisor reviews each plan for legal considerations, appropriate goals in accordance with the collection objectives of the supported unit, and makes any changes he thinks are necessary. The supervisor ensures that contract interrogators are utilized in accordance with the scope of their contract and current policy. (See Appendix K.) After the plan is approved, the collection operation is executed. Prior to execution, the supervisor ensures mission brief back, rehearsal, and pre-combat inspections are conducted.

Chapter 8

Approach Techniques and Termination Strategies

8-1. Regardless of the type of operation, the initial impression that the HUMINT collector makes on the source and the approach he takes to gain the source's cooperation will have a lasting effect on the continuing relationship and the degree of success in collecting information. The approach used will vary based on the type of operation; the operational environment; the status of the source; the personality, position, and identity of the source; and the personality and experience level of the HUMINT collector and the time available.

8-2. The MPs will not take any actions to set conditions for interrogations (for example, "softening up" a detainee). Additionally, in accordance with DOD Directive 3115.09, military working dogs, contracted dogs, or any other dog in use by a government agency shall not be used as a part of an interrogation approach nor to harass, intimidate, threaten, or coerce a detainee for interrogation purposes. Leadership throughout the chain of command is responsible to ensure that HUMINT operations are in compliance with these governing regulations and guidelines, whether the HUMINT collection is to take place as part of HCT operations or in an internment facility.

8-3. The only authorized interrogation approaches and techniques are those authorized by and listed in this manual, in accordance with the Detainee Treatment Act of 2005. Two approaches, Mutt and Jeff and False Flag, require approval by the first O-6 in the interrogator's chain of command. The restricted interrogation technique "Separation" requires COCOM commander approval for use, and approval of each interrogation plan using "Separation" by the first General Officer/Flag Officer (GO/FO) in the chain of command. Coordination may also be required with the C/J/G2X, security, legal, or other personnel. Regardless of the coordination efforts required, use of all techniques at all locations must carefully comply with this manual and additional instructions contained in the latest DOD and COCOM policies.

NOTE: The word "source" will be used in this chapter to mean any person who is the objective of the HUMINT collector's approach, and is applicable in any collection situation unless otherwise noted in the text. This use of the term "source" is consistent with US Army Intelligence Center HUMINT collector training.

APPROACH PHASE

8-4. During the approach phase, the HUMINT collector establishes the conditions of control and rapport to facilitate information collection. The approach begins with initial contact between the source and the HUMINT collector. Extreme care is required since the success of the collection effort

hinges, to a large degree, on the early development of the source's willingness to communicate. Interrogators must have a deep understanding of the cultural norms, anomalies, and emotional triggers of the person being interrogated in order to select appropriate approach strategies and to interrogate effectively.

8-5. The HUMINT collector's objective during this phase is to establish a relationship with the source that results in the source providing accurate and reliable information in response to the HUMINT collector's questions. The HUMINT collector adopts an appropriate persona based on his appraisal of the source but remains alert for verbal and non-verbal clues that indicate the need for a change in the approach techniques. The amount of time spent on this phase will depend mostly on the probable quantity and value of information the source possesses, the availability of other sources with knowledge on the same topics, and available time. At the initial contact, a businesslike relationship should be maintained. As the source assumes a cooperative attitude, a more relaxed atmosphere may be advantageous. The HUMINT collector must carefully determine which of the various approach techniques to employ.

8-6. Sources will cooperate with the HUMINT collector for various reasons ranging from patriotic duty to personal gain, such as material gifts or money. They may also respond to emotion or logic. Regardless of the type of source and his outward personality, every source possesses exploitable characteristics that, if recognized by the HUMINT collector, can be used to facilitate the collection process. These characteristics may be readily apparent or may have to be extrapolated from the source's speech, mannerisms, facial expressions, physical movements, involuntary responses (perspiration, changes in breathing, eye movement), and other overt indications that vary from source to source. From a psychological standpoint, the HUMINT collector must be cognizant of the following behaviors. People tend to—

- Want to talk when they are under stress and respond to kindness and understanding during trying circumstances. For example, enemy soldiers who have just been captured have experienced a significant stress-producing episode. The natural inclination is for people to want to talk about this sort of experience. If the EPW has been properly segregated and silenced, the HUMINT collector will be the first person the EPW has a chance to talk to. This is a powerful tool for the collector to use to get the subject talking. The desire to talk may also be manifested in refugees, DPs, and even local civilians when confronted by an unsettled situation.
- Show deference when confronted by superior authority. This is culturally dependent but in most areas of the world people are used to responding to questions from a variety of government and quasi-government officials.
- Operate within a framework of personal and culturally derived values. People tend to respond positively to individuals who display the same value system and negatively when their core values are challenged.
- Respond to physical and, more importantly, emotional self-interest. This may be as simple as responding to material rewards such as extra

food or luxury items for their personal comfort or as complex as responding to support in rationalizing guilt.

- Fail to apply or remember lessons they may have been taught regarding security if confronted with a disorganized or strange situation.
- Be more willing to discuss a topic about which the HUMINT collector demonstrates identical or related experience or knowledge.
- Appreciate flattery and exoneration from guilt.
- Attach less importance to a topic if it is treated routinely by the HUMINT collector.
- Resent having someone or something they respect belittled, especially by someone they dislike.

8-7. HUMINT collectors do not "run" an approach by following a set pattern or routine. Each approach is different, but all approaches have the following in common. They—

- Establish and maintain control over the source and collection effort. This does not necessarily equate to physical control. Rather it means that the HUMINT collector directs the conversation to cover the topics that are of interest to him. This may be overt in a debriefing or an interrogation or subtle in an elicitation. In a very basic sense, the HUMINT collector is in control if he is asking questions and receiving answers. If the source is asking questions, refusing to answer questions, or directing or attempting to direct the exchange, he is challenging for control. If the source challenges this control, the HUMINT collector must act quickly and firmly to reestablish control.
- Establish and maintain a rapport between the HUMINT collector and the source. Rapport is a condition established by the HUMINT collector that is characterized by source confidence in the HUMINT collector and a willingness to cooperate with him. This does not necessarily equate to a friendly atmosphere. It means that a relationship is established and maintained that facilitates the collection of information by the HUMINT collector. The HUMINT collector may establish a relationship as superior, equal, or even inferior to the source. The relationship may be based on friendship, mutual gain, or even fear.
- Identify the source's primary emotions, values, traditions, and characteristics and use them to gain the source's willing cooperation.

8-8. The successful application of approach techniques, coupled with measures to ensure source veracity, results in the source providing accurate information in response to the HUMINT collector's requirements. The source may or may not be aware that he is providing the HUMINT collector with needed information. The approach does not end when the source begins providing information but is reinforced as necessary throughout the questioning.

DEVELOPING RAPPORT

8-9. The basis of rapport is source confidence in the HUMINT collector, which leads to a willingness to cooperate. Rapport does not necessarily mean a friendly relationship, although that may be the case. It means an establishment of a relationship in which the HUMINT collector presents a realistic persona designed to evoke cooperation from the source. The source responds with relevant, truthful information. Rapport is established during the approach and must be maintained throughout the questioning of the source. If the HUMINT collector has established good rapport initially and then abandons the effort, the source would rightfully begin to question the HUMINT collector's sincerity and may cease answering questions.

BUILDING RAPPORT

8-10. Building rapport is an integral part of the approach phase. The establishment of rapport begins when the HUMINT collector first encounters the source. Depending on the situation, the HUMINT collector may introduce himself to the source. In debriefing and liaison operations, this will normally be the collector's true name and affiliation. In elicitation, the requirement and type of introduction depends on the operation. In interrogation operations, the HUMINT collector normally will not introduce himself unless he is laying the groundwork for an approach. If he does introduce himself, normally he will adopt a duty position and rank supportive of the approach strategy selected during the planning and preparation phase. The HUMINT collector must select a rank and duty position that is believable based on the HUMINT collector's age, appearance, and experience. A HUMINT collector may, according to international law, use ruses of war to build rapport with interrogation sources, and this may include posing or "passing himself off" as someone other than a military interrogator. However, the collector must not pose as—

- A doctor, medic, or any other type of medical personnel.
- Any member of the International Committee of the Red Cross (ICRC) or its affiliates. Such a ruse is a violation of US treaty obligations.
- A chaplain or clergyman.
- A journalist.
- A member of the US Congress.

8-11. The HUMINT collector should seek advice from his SJA concerning representing himself as holding any other sensitive position.

8-12. A good source assessment is the basis for the approach and vital to the success of the collection effort. The HUMINT collector continually assesses the source to see if the approaches—and later the questioning techniques—chosen in the planning and preparation phase will indeed work. Approaches chosen in planning and preparation are tentative and based on the limited information available from documents, guards, and personal observation. This may lead the HUMINT collector to select approaches that may be totally incorrect for obtaining this source's willing cooperation. Thus, careful assessment of the source is critical to avoid wasting valuable time in the approach phase. Whether the HUMINT collector is using reasoned argument

or emotion to get the source to cooperate, he must be convincing and believable and appear sincere.

RAPPORT POSTURE

8-13. Unless there is rationale for acting otherwise, the HUMINT collector will begin his interaction with the source in a businesslike manner. He will be neither hostile nor overly friendly. Based on the tentative approaches developed during planning and preparation and the verbal and physical clues from the source, the HUMINT collector will modify this posture to facilitate collection.

8-14. Based on planning and preparation, the HUMINT collector may decide to adopt a stern posture. He presents himself as a person in a superior position to the interrogation source and demands proper deference and obedience by the interrogation source. In the case of an EPW this is manifested by having the source remain at attention and address the HUMINT collector as "Sir." This can be effective in dealing with lower ranking military personnel or members of oppressed ethnic, tribal, or religious groups who are conditioned to respond to authority or civilians in lower economic or social positions who are used to responding to directions from various bureaucrats and civilian superiors. This posture can have negative results since many persons in the positions mentioned above have developed mechanisms for dealing with superiors that mostly involve giving minimal information and agreeing with whatever the authority figure says.

8-15. In most cases, either initially or after the interrogation source has begun answering questions, the HUMINT collector will adopt a more relaxed or even sympathetic posture. The HUMINT collector addresses the interrogation source in a friendly fashion, striving to put him at ease. Regardless of the posture selected by the HUMINT collector, he must stay detached emotionally while maintaining the appearance of total involvement and stay within his adopted persona. The HUMINT collector must control his temper at all times. He must not show distaste, disgust, or unease at anything the source says unless that reaction is a planned part of the approach strategy. He should not show surprise at anything that the interrogation source says since it might undermine source confidence in the HUMINT collector and their relationship.

8-16. The HUMINT collector must support his verbal approaches with appropriate body language. Just as the HUMINT collector is observing the source to identify non-verbal clues that support or contradict the verbal message, the HUMINT collector is being scrutinized by the source to identify the same clues. The techniques used in an approach are a totality of effort, not just verbal conversation between the HUMINT collector and the source. Body language is in many instances culturally dependent. Standing at a given distance from an individual may be perceived as comforting in some societies and hostile in others. The HUMINT collector must adapt his body language to the culture in which he is working rather than expect the source to adapt to his.

APPROACH TECHNIQUES

8-17. The approaches listed are not guaranteed solutions for every situation. Some individual approaches that may be suitable for one operating environment, such as when conducting HUMINT contact operations, may be ineffective in another, such as interrogation. Some will be successful with one source and ineffective with another. In any case, everything the HUMINT collector says and does must be in compliance with the applicable law and policy under which the HUMINT collector is operating. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs.

8-18. There are 18 approach techniques that can be employed on any detainee regardless of status or characterization, including EPWs. Additionally, there is one restricted interrogation technique called separation (see Appendix M). Separation cannot be employed on EPWs. With the exception of the direct approach, which may be effective by itself, approach techniques are used in combination with other approaches and techniques. Transitions from one approach to another must be smooth, logical, and convincing.

DIRECT APPROACH

8-19. (Interrogation and Other MSO) Almost all HUMINT collection begins with the direct approach. The exception to this is during elicitation operations that by their very nature are indirect. In using the direct approach, the HUMINT collector asks direct questions (see Chapter 9). The initial questions may be administrative or nonpertinent but the HUMINT collector quickly begins asking pertinent questions. The HUMINT collector will continue to use direct questions as long as the source is answering the questions in a truthful manner. When the source refuses to answer, avoids answering, or falsely answers a pertinent question, the HUMINT collector will begin an alternate approach strategy. The fact that the source is answering questions does not preclude the HUMINT collector from providing an incentive to reward the source and continue his cooperation as long as that incentive does not slow down the collection. For example, a HUMINT collector might offer the source coffee or cigarettes to reward his cooperation. See Chapter 9 for the use of Repeat and Control questions in detecting deception.

8-20. Statistics from interrogation operations in World War II show that the direct approach was effective 90 percent of the time. In Vietnam and in Operations URGENT FURY (Grenada, 1983), JUST CAUSE (Panama, 1989), and DESERT STORM (Kuwait and Iraq, 1991), the direct approach was 95 percent effective. The effectiveness of the direct approach in Operations ENDURING FREEDOM (Afghanistan, 2001-2002) and IRAQI FREEDOM (Iraq, 2003) are still being studied; however, unofficial studies indicate that in these operations, the direct approach has been dramatically less successful. The direct approach is frequently employed at lower echelons when the tactical situation precludes selecting other techniques, and where

the EPW's or detainee's mental state is one of confusion or extreme shock. However, the HUMINT collector must remember that just because a source is answering a direct question does not mean he is being truthful.

INCENTIVE APPROACH

8-21. (Interrogation and Other MSO) The incentive approach is trading something that the source wants for information. The thing that you give up may be a material reward, an emotional reward, or the removal of a real or perceived negative stimulus. The exchange of the incentive may be blatant or subtle. On one extreme, the exchange may be a formal cash payment for information during some contact operations while on the other extreme it may be as subtle as offering the source a cigarette. Even when the direct approach is successful, the HUMINT collector may use incentives to enhance rapport and to reward the source for cooperation and truthfulness. The HUMINT collector must be extremely careful in selecting the options offered to a detainee source. He cannot deny the detainee anything that he is entitled to by law.

8-22. The HUMINT collector also should not offer anything that is not in his power to give. Although this might be expedient in the short term, in the long run it will eliminate source cooperation. When asked to provide something beyond his authority, the HUMINT collector can agree to help, check into, or otherwise support the request without committing himself to its successful accomplishment. HUMINT collectors must be cautious in the use of incentives for the following reasons:

- There is an inherent suspicion of the truthfulness of "bought" information. Sources may manufacture information in order to receive or maintain an incentive. Sources may also "hold back" information in the hopes of trading it at a later date for greater incentives. They may also hold back information if the incentive is not immediately available or guaranteed.
- The incentive must be believable and attainable. The incentive must be within the capability of the HUMINT collector's assumed persona to achieve. For example, if the detainee was captured after killing a US soldier, an incentive of release would not be realistic or believable. Likewise, if the interrogator is presenting himself as being a "harmless clerk" at the detention center, it would be unrealistic to expect a detainee to believe that a clerk could arrange to have the detainee's girlfriend brought to visit him. Such a visit might be possible, but the interrogator's assumed persona would not seemingly provide him with the authority to make it happen.
- The HUMINT collector must provide any promised incentive. A simple promise of an incentive may be sufficient to obtain immediate cooperation. If, however, the HUMINT collector does not follow through on providing the incentive, he will lose credibility and rapport with his source. This may end the cooperation of not only that source but also possibly any potential source who has contact with that source.
- The HUMINT collector may not state or even imply that the basic human rights guaranteed by applicable national and international

laws, regulations, and agreements will be contingent on a detained source's cooperation. An incentive for cooperation is viable only if the HUMINT collector has or is perceived to have the authority to withhold the incentive if the source is not cooperative. A HUMINT collector cannot promise an EPW that he will be treated in accordance with the GPW if he cooperates. This statement implies that the EPW will not be treated properly if he does not cooperate. Since the EPW must be treated in accordance with the GPW whether he cooperates or not, the HUMINT collector will rapidly lose credibility.

EMOTIONAL APPROACHES

8-23. (Interrogation and Other MSO) Emotional approaches are centered on how the source views himself and his interrelationships with others. Through source observation and initial questioning, the HUMINT collector can often identify dominant emotions that motivate the EPW/detainee. The motivating emotion may be greed, love, hate, revenge, or others. The emotion may be directed inward (feelings of pride or helplessness) or outward (love of family). The HUMINT collector employs verbal and emotional ruses in applying pressure to the source's dominant emotions. He then links the satisfaction of these emotions to the source's cooperation. Often, the presentation of like experiences and presenting the source with an opportunity to express his emotions is sufficient to result in cooperation. However, sometimes the source must be presented with a specific action or tangible manifestation of support.

8-24. Although the emotion is the key factor, an emotional approach is normally worthless without an attached incentive. The incentive must meet the criteria listed above for the incentive approach to ensure that the incentive is believable and attainable. For example, this technique can be used on the EPW/detainee who has a great love for his unit and fellow soldiers. Simply having the source express this emotion is not enough. After the source expresses this emotion, the HUMINT collector can take advantage of this by telling the EPW/detainee that by providing pertinent information, he may shorten the war or battle in progress and save many of his comrades' lives, but his refusal to talk may cause their deaths. This gives the source the alternatives of facing the status quo or expressing love of comrades through cooperating with the HUMINT collector.

8-25. Religion is an especially difficult topic to use in any emotional approach. An approach using religion may encourage the source to be further motivated by love, remorse, futility, or even pride to cooperate with the interrogator. On the other hand, an approach using religion may also encourage the source to end any rapport and cooperation with the interrogator. Although it is acceptable to use religion in all interrogation approaches, even to express doubts about a religion, an interrogator is not permitted to denigrate a religion's symbols (for example, a Koran, prayer rug, icon, or religious statue) or violate a religion's tenets, except where appropriate for health, safety, and security reasons. Supervisors should carefully consider the experience level of their subordinates before permitting the use of religion in any interrogation approach.

8-26. Similarly, supervisors should question the appropriateness of demeaning any racial group, including the source's, to elicit an emotional response during an interrogation approach.

8-27. One common danger to the use of emotional approaches is the development of an emotional attachment on the part of the HUMINT collector. It is natural that a source will develop an emotional attachment to the HUMINT collector. The HUMINT collector will often foster this attachment. However, it is vital the HUMINT collector not develop a corresponding emotional attachment to the source. This problem normally develops when a HUMINT collector has contact with one source or a group of similar sources over an extended period of time. There is transference of the source's problems to the HUMINT collector. For example, HUMINT collectors working in a refugee camp frequently begin to view the welfare of the refugees as a greater concern than HUMINT collection. The HUMINT collector, while developing emotion within the source, must act believably but at the same time he must remain detached. He must remember that the emotion is a means to an end (that is, information collection). Supervisors must carefully observe HUMINT collectors for signs of this emotional attachment to the source and take appropriate action ranging from counseling to reassignment.

8-28. The following are types of emotional approaches.

Emotional Love Approach

8-29. (Interrogation and Other MSO) Love in its many forms (friendship, comradeship, patriotism, love of family) is a dominant emotion for most people. The HUMINT collector focuses on the anxiety felt by the source about the circumstances in which he finds himself, his isolation from those he loves, and his feelings of helplessness. The HUMINT collector directs the love the source feels toward the appropriate object: family, homeland, or comrades. If the HUMINT collector can show the source what the source himself can do to alter or improve his situation or the situation of the object of his emotion, the approach has a chance of success.

8-30. The key to the successful use of this approach is to identify an action that can realistically evoke this emotion (an incentive) that can be tied to a detained source's cooperation. For example, if the source cooperates, he can see his family sooner, end the war, protect his comrades, help his country, help his ethnic group. A good HUMINT collector will usually orchestrate some futility with an emotional love approach to hasten the source's reaching the breaking point. In other words if the source does not cooperate, these things may never happen or be delayed in happening. Sincerity and conviction are critical in a successful attempt at an emotional love approach as the HUMINT collector must show genuine concern for the source, and for the object at which the HUMINT collector is directing the source's emotion. The emotional love approach may be used in any MSO where the source's state of mind indicates that the approach may be effective.

Emotional Hate Approach

8-31. (Interrogation and Other MSO) The emotional hate approach focuses on any genuine hate, or possibly a desire for revenge, the source may feel. The HUMINT collector must clearly identify the object of the source's hate and, if necessary, build on those feelings so the emotion overrides the source's rational side. The source may have negative feelings about his country's regime, immediate superiors, officers in general, or fellow soldiers. The emotional hate approach may be used in any MSO where the source's state of mind indicates that the approach may be effective.

8-32. The emotional hate approach may be effective on members of racial or religious minorities who have or feel that they have faced discrimination in military and civilian life. The "hate" may be very specific. For example, a source may have great love for his country, but may hate the regime in control. The HUMINT collector must be sure to correctly identify the specific object of the hate. The emotional hate approach is most effective with the immature or timid source who may have had no opportunity up to this point for revenge, or never had the courage to voice his feelings.

8-33. As in the emotional love approach, the key to the successful application is the linking of the emotion with a tangible manifestation of that emotion. The HUMINT collector must be extremely careful that he does not promise anything that would be contrary to national or international law or US interests or goals. For example, if an EPW feels he has been treated unfairly in his unit, the HUMINT collector can point out that, if the source cooperates and divulges the location of that unit, the unit can be destroyed, thus affording the source revenge. But he cannot promise that the unit if attacked would not be allowed to surrender or that the unit if it surrenders will be treated badly.

8-34. The HUMINT collector must be careful that he does not assume that casual negative comments equate to a strong hate. Many soldiers will make negative comments against their army but will support and defend their army against any "outsider." The HUMINT collector should also not assume generalities; for example, assuming that a member of an ethnic minority hates the ethnic majority just because most ethnic minorities hate those in the ethnic majority.

Emotional Fear-Up Approach

8-35. (Interrogation and Other MSO) Fear is another dominant emotion that can be exploited by the HUMINT collector. In the fear-up approach, the HUMINT collector identifies a preexisting fear or creates a fear within the source. He then links the elimination or reduction of the fear to cooperation on the part of the source. The HUMINT collector must be extremely careful that he does not threaten or coerce a source. Conveying a threat may be a violation of the UCMJ. The HUMINT collector should also be extremely careful that he does not create so much fear that the source becomes unresponsive. The HUMINT collector should never act as if he is out of control or set himself up as the object or focal point of the source's fear. If the HUMINT collector acts in this manner, it is extremely difficult to then act as

the outlet for the fear. Supervisors should consider the experience level of their subordinates before approving their use of this approach.

8-36. If there is a justifiable fear, the HUMINT collector should present it and present a plan to mitigate it if the source cooperates (combination of emotional and incentive approaches). For example, an EPW source says that he will not cooperate because if he does his fellow prisoners will kill him or, if a contact source says that if people find out he is cooperating, his family will suffer. In these cases, the HUMINT collector can point out that the source has already placed himself at risk and he or his family may suffer whether he cooperates or not (justified fear). But if he cooperates, the HUMINT collector will do his best to ensure that either no one will find out or that he will be protected (incentive).

8-37. If there is no justified fear, the HUMINT collector can make use of non-specific fears. "You know what can happen to you here?" A fear-up approach is normally presented in a level, unemotional tone of voice. For example, "We have heard many allegations of atrocities committed in your area and anyone that was involved will be severely punished" (non-specific fear). "If you cooperate with me and answer all of my questions truthfully, I can make sure you are not falsely accused" (incentive). The source should demonstrate some indication of fear, whether verbal or non-verbal, prior to using this approach. If a fear is pre-existing, the approach will work and is legal. If there is no indication of fear, another approach should be considered.

8-38. It is often very effective to use the detainee's own imagination against him. The detainee can often visualize exactly what he is afraid of better than the HUMINT collector can express it.

8-39. The "fear-up" approach is frequently used in conjunction with the emotional love or hate approaches. For example, the HUMINT collector has already established that a detainee source has a strong love of family but is now separated from them. He may state, "I wonder how your family is getting along without you?" (fear of the unknown). He then promises to allow the detainee more than the minimum two letters a month required by the GPW.

Emotional Fear-Down Approach

8-40. (Interrogation and Other MSO) The emotion of fear may dominate the source to the point where he is unable to respond rationally to questioning, especially in interrogation sources. However, the fear-down approach may be used in any MSO where the source's state of mind indicates that it would be an appropriate approach to use. In the fear-down approach the HUMINT collector mitigates existing fear in exchange for cooperation on the part of the source. This is not normally a formal or even voiced agreement. Instead, the HUMINT collector through verbal and physical actions calms the source. Psychologically, the source then views the HUMINT collector as the protector or the one who is providing the calm and wishes to help the HUMINT collector in gratitude and in order to maintain the HUMINT collector as the protector. When used with a soothing, calm tone of voice and appropriate body language, a fear-down approach often creates rapport and nothing else may be needed to get the source to cooperate. At times, however, the

HUMINT collector must describe concrete actions that he will take in order to remove the source's fear.

8-41. Frequently the object of the fear is too traumatic for the source to face directly. While calming the source, the HUMINT collector may initially ask nonpertinent questions and avoid the subject that has caused the source's fear. This develops rapport and establishes communication. The HUMINT collector must remember that his goal is collecting information, not concern with the psychological well being of the source. He will be concerned with the latter only insofar as it helps him obtain the former. This approach technique may backfire if allowed to go too far. After convincing the source he has nothing to fear, the source may cease to be afraid and may feel secure enough to resist the HUMINT collector's pertinent question.

Emotional-Pride and Ego-Up Approach

8-42. (Interrogation and Other MSO) The emotional-pride and ego-up approach may be used in any MSO. It exploits a source's low self-esteem. Many HUMINT sources including EPWs and other detainees, retained persons, civilian internees, or refugees may suffer from low self-esteem and feelings of helplessness due to their immediate circumstances. Others, such as individuals or members of social or ethnic groups that have been discriminated against or low-ranking members of organizations (including the military), may also show low self-worth. In this technique, the source is flattered into providing certain information in order to gain credit and build his ego. The HUMINT collector must take care to use a flattering somewhat-in-awe tone of voice, and speak highly of the source throughout this approach while remaining believable. This should produce positive feelings on the source's part as he receives desired recognition. The source will eventually reveal pertinent information to solicit more favorable comments from the HUMINT collector.

8-43. This technique can also be employed in another manner—by flattering the source into admitting certain information in order to gain credit. For example, while interrogating a suspected saboteur, the HUMINT collector states: "This was a smooth operation. I have seen many previous attempts fail. I bet you planned this. Who else but a clever person like you would have planned it? When did you first decide to do the job?"

8-44. A variation of this approach can also be used on individuals with strong egos. It is based on the premise that everyone likes to talk about what they do best. The HUMINT collector shows interest in and asks the source to explain an aspect of his job. The questioning begins with nonpertinent aspects of the source's job. The HUMINT collector displays interest and asks increasingly technical and pertinent questions. For example, if the source is an EPW who was a pilot, the HUMINT collector might begin by asking him what it is like to fly. As the source talks about this, the collector demonstrates interest and gradually uses questions to lead the conversation to capabilities of specific aircraft, specific missions that the pilot has flown, tactics, or whatever topic is a priority for collection.

Emotional-Pride and Ego-Down Approach

8-45. (Interrogation) The emotional-pride and ego-down approach is based on attacking the source's ego or self-image. The source, in defending his ego, reveals information to justify or rationalize his actions. This information may be valuable in answering collection requirements or may give the HUMINT collector insight into the viability of other approaches. This approach is effective with sources who have displayed weakness or feelings of inferiority. A real or imaginary deficiency voiced about the source, loyalty to his organization, or any other feature can provide a basis for this technique.

8-46. The HUMINT collector accuses the source of weakness or implies he is unable to do a certain thing. This type of source is also prone to excuses and rationalizations, often shifting the blame to others. An example of this technique is opening the collection effort with the question, "Why did you surrender so easily when you could have escaped by crossing the nearby ford in the river?" The source is likely to provide a basis for further questions or to reveal significant information if he attempts to explain his surrender in order to vindicate himself. He may give an answer such as, "No one could cross the ford because it is mined."

8-47. The objective is for the HUMINT collector to use the source's sense of pride by attacking his loyalty, intelligence, abilities, leadership qualities, slovenly appearance, or any other perceived weakness. This will usually goad the source into becoming defensive, and he will try to convince the HUMINT collector he is wrong. In his attempt to redeem his pride and explain his actions, the source may provide pertinent information. Possible targets for the emotional-pride and ego-down approach are the source's—

- Loyalty.
- Technical competence.
- Leadership abilities.
- Soldierly qualities.
- Appearance.

8-48. There is a risk associated with this approach. If the emotional-pride and ego-down approach fails, it is difficult for the HUMINT collector to recover and move to another approach without losing his credibility. Also, there is potential for application of the pride and ego approach to cross the line into humiliating and degrading treatment of the detainee. Supervisors should consider the experience level of their subordinates and determine specifically how the interrogator intends to apply the approach technique before approving the interrogation plan.

Emotional-Futility

8-49. (Interrogation and Other MSO) The emotional-futility approach is generally used in an interrogation setting, but may also be used for other MSO, if indicated by the source's state of mind. In the emotional-futility approach, the HUMINT collector convinces the source that resistance to questioning is futile. This engenders a feeling of hopelessness and helplessness on the part of the source. Again as with the other emotional approaches, the HUMINT collector gives the source a "way out" of the

helpless situation. For example "it is hopeless for your forces to continue fighting because they can no longer get supplies, but you can help end the war and their suffering." When employing this technique, the HUMINT collector must have factual information. The HUMINT collector presents these facts in a persuasive, logical manner. He should be aware of and able to exploit the source's psychological and moral weaknesses, as well as weaknesses inherent in his society.

8-50. The futility approach is effective when the HUMINT collector can play on doubts that already exist in the source's mind. Factual or seemingly factual information must be presented in a persuasive, logical manner, and in a matter-of-fact tone of voice. Making the situation appear hopeless allows the source to rationalize his actions, especially if that action is cooperating with the HUMINT collector. When employing this technique, the HUMINT collector must not only have factual information but also be aware of and exploit the source's psychological, moral, and sociological weaknesses. Another way of using the futility approach is to blow things out of proportion. If the source's unit was low on, or had exhausted, all food supplies, he can be easily led to believe all of his forces had run out of food. If the source is verging on cooperating, it may aid the collection effort if he is told all the other sources have cooperated.

8-51. The futility approach must be orchestrated with other approach techniques (for example, love of comrades). A source who may want to help save his comrades' lives may be convinced the battlefield situation is hopeless and they will die without his assistance. The futility approach is used to paint a bleak picture for the prisoner, but it is not normally effective in and of itself in gaining the source's cooperation.

Other Approaches

8-52. There are numerous other approaches but most require considerable time and resources. Most are more appropriate for use with sources who are detainees, but some, such as change of scenery, may have application for elicitation or MSO.

8-53. **We Know All**. (Interrogation) In the "we know all" approach technique, the HUMINT collector subtly convinces the source that his questioning of the source is perfunctory because any information that the source has is already known. This approach may be employed in conjunction with the "file and dossier" technique or by itself. If used alone, the HUMINT collector must first become thoroughly familiar with available data concerning the source and the current situation. To begin the collection effort, the HUMINT collector asks questions based on this known data.

8-54. When the source hesitates, refuses to answer, or provides an incorrect or incomplete reply, the HUMINT collector provides the detailed answer himself. The HUMINT collector may even complete a source's answer, as if he is bored and just "going through the motions." When the source begins to give accurate and complete information, the HUMINT collector interjects pertinent questions. Questions to which answers are already known are also asked periodically to test the source's truthfulness and to maintain the deception that the information is already known. There are some inherent

problems with the use of the "we know all" approach. The HUMINT collector is required to prepare everything in detail, which is time consuming. He must commit much of the information to memory, as working from notes may show the limits of the information actually known. It is also only usable when sufficient prior information exists to convince the source that "we know all."

8-55. **File and Dossier**. (Interrogation) The file and dossier approach is a variation of the "we know all" approach. The HUMINT collector prepares a dossier containing all available information concerning the source or his organization. The information is carefully arranged within a file to give the illusion that it contains more data than actually there. The file may be padded with extra paper if necessary. Index tabs with titles such as education, employment, criminal record, military service, and others are particularly effective. It is also effective if the HUMINT collector is reviewing the dossier when the source enters the room and the source is able to read his name on the dossier and sees the numerous topics and supposed extent of the files.

8-56. The HUMINT collector proceeds as in the "we know all" approach. He refers to the particular labeled segment of the dossier before, during, or after asking a question. In the early stages of questioning, the HUMINT collector asks questions to which he has the answer. He may answer along with the source, complete the information for the source, or even show the source where the information is entered in the dossier. He never lets the source physically handle the dossier. As the source becomes convinced that all the information that he knows is contained within the dossier, the HUMINT collector proceeds to topics on which he has no or little information. In doing so, he still refers to the appropriate section of the dossier and may even nod his head knowingly or tell the source that the information the source is providing still matches what is in the dossier.

8-57. This technique has several limitations and drawbacks. The preparation time in developing the dossier is extensive. The success of this technique is largely dependent on the naiveté of the source, volume of data on the subject, and skill of the HUMINT collector in convincing the source that the dossier is more complete than it actually is. There is also the risk that a less naïve source will refuse to cooperate, claiming that, if the collector already knows everything, there is no need for him to talk. Also with this technique, the HUMINT collector is limited in the method he may use to record new information. If the HUMINT collector writes down information, it destroys the illusion that all the information has already been obtained. The HUMINT collector is normally limited to using electronic recording devices or his memory. The HUMINT collector can also arrange ahead of time for another interrogator or analyst to take notes for him, undetected by the source. This could be especially effective in a situation where a separate monitoring area (for oversight) is used by the analyst.

8-58. **Establish Your Identity**. (Interrogation) In using this approach, the HUMINT collector insists the detained source has been correctly identified as an infamous individual wanted by higher authorities on serious charges, and he is not the person he purports to be. In an effort to clear himself of this

allegation, the source makes a genuine and detailed effort to establish or substantiate his true identity. In so doing, he may provide the HUMINT collector with information and leads for further development. The HUMINT collector should initially refuse to believe the source and insist he is the individual wanted by the ambiguous higher authorities. This will force the source to give even more detailed information in order to convince the HUMINT collector he is who he says he is.

8-59. **Repetition**. (Interrogation) The repetition approach is used to induce cooperation from a hostile source. In one variation of this approach, the HUMINT collector listens carefully to a source's answer to a question, and then repeats the question and answer several times. He does this with each succeeding question until the source becomes so thoroughly bored with the procedure, he answers questions fully and candidly to satisfy the HUMINT collector and gain relief from the monotony of this method. The repetition technique must be judiciously used, as it will generally be ineffective when employed against introverted sources or those having great self-control. It may also provide an opportunity for a source to regain his composure and delay the collection effort. In this approach, the use of more than one HUMINT collector or a tape recorder has proven effective.

8-60. **Rapid Fire**. (Interrogation) The rapid-fire approach is based upon the principles that—

- Everyone likes to be heard when he speaks.
- It is confusing to be interrupted in mid-sentence with an unrelated question.

8-61. This approach may be used by one, two, or more HUMINT collectors to question the source. In employing this technique, the HUMINT collectors ask a series of questions in such a manner that the source does not have time to answer a question completely before the next one is asked. This confuses the source, and he will tend to contradict himself as he has little time to formulate his answers. The HUMINT collectors then confront the source with the inconsistencies causing further contradictions. In many instances, the source will begin to talk freely in an attempt to explain himself and deny the HUMINT collector's claims of inconsistencies. In this attempt, the source is likely to reveal more than he intends, thus creating additional leads for further exploitation. This approach may be orchestrated with the emotional-pride and ego-down or fear-up approaches. Besides extensive preparation, this approach requires experienced and competent HUMINT collectors, with comprehensive case knowledge and fluency in the source's language.

8-62. **Silent**. (Interrogation) The silent approach may be successful when used against either a nervous or confident source. When employing this technique, the HUMINT collector says nothing to the source, but looks him squarely in the eye, preferably with a slight smile on his face. It is important not to look away from the source but force him to break eye contact first. The source may become nervous, begin to shift in his chair, cross and re-cross his legs, and look away. He may ask questions, but the HUMINT collector should not answer until he is ready to break the silence. The source may blurt out questions such as, "Come on now, what do you want with me?" When the HUMINT collector is ready to break silence, he may do so with questions

such as, "You planned this operation for a long time, didn't you? Was it your idea?" The HUMINT collector must be patient when using this technique. It may appear the technique is not succeeding, but usually will when given a reasonable chance.

8-63. **Change of Scenery**. (Interrogation and Other MSO) The change-of-scenery approach may be used in any type of MSO to remove the source from an intimidating atmosphere such as an "interrogation" room type of setting and to place him in a setting where he feels more comfortable speaking. Bringing a source into a formal setting to conduct an interrogation or debriefing has psychological implications. On the positive side, it places the HUMINT collector in a superior position since he is operating on his "home turf" and has set the conditions for the meeting. It allows the HUMINT collector control over the immediate environment including the positioning of the participants, to establish the desired atmosphere for the approach.

8-64. However, there are potential negative factors in the conduct of questioning in an "Interrogation Room" environment. The source may be intimidated and more guarded; he may consider the formal setting in terms of an adversarial relationship; and he may limit his answers as a mode of self-protection. In some circumstances, the HUMINT collector may be able to invite the source to a different setting for coffee and pleasant conversation. When removed from the formal environment, the source may experience a feeling of leaving the interrogation behind. The perceived reduced pressure may lower his guard and allow him to attach less significance to conversation that occurs outside the formal setting, even though pertinent information is still being discussed. During the conversation in this more relaxed environment, the HUMINT collector steers the conversation to the topic of interest. Through this somewhat indirect method, he attempts to elicit the desired information. The source may never realize he is still being questioned.

8-65. **Mutt and Jeff. (Interrogation)** The goal of this technique is to make the source identify with one of the interrogators and thereby establish rapport and cooperation. This technique involves a psychological ploy that takes advantage of the natural uncertainty and guilt that a source has as a result of being detained and questioned. Use of this technique requires two experienced HUMINT collectors who are convincing actors. The two HUMINT collectors will display opposing personalities and attitudes toward the source. For example, the first HUMINT collector is very formal and displays an unsympathetic attitude toward the source. He may, for instance, be very strict and order the source to follow all military courtesies during questioning. Although he conveys an unfeeling attitude, the HUMINT collector is careful not to threaten or coerce the source. Conveying a threat of violence is a violation of the UCMJ.

8-66. At the point when the interrogator senses the source is vulnerable, the second HUMINT collector appears (having received his cue by a signal, hidden from the source, or by listening and observing out of view of the source), and scolds the first HUMINT collector for his uncaring behavior and orders him from the room. The second HUMINT collector then apologizes to soothe the source, perhaps offering him a beverage and a cigarette. He

explains that the actions of the first HUMINT collector were largely the result of an inferior intellect and lack of sensitivity. The inference is that the second HUMINT collector and the source share a high degree of intelligence and sensitivity.

8-67. The source is normally inclined to have a feeling of gratitude towards the second HUMINT collector, who continues to show sympathy in an effort to increase rapport and control for the questioning that will follow. If the source's cooperation begins to fade, the second HUMINT collector can hint that he is a busy person of high rank, and therefore cannot afford to waste time on an uncooperative source. He can broadly imply that the first HUMINT collector might return to continue the questioning. The Mutt and Jeff approach may be effective when orchestrated with Pride and Ego Up and Down, Fear Up and Down, Futility, or Emotional Love or Hate.

8-68. **Oversight Considerations:** Planned use of the Mutt and Jeff approach must be approved by the first O-6 in the interrogator's chain of command. The HUMINT collector must include as a part of the interrogation plan—

- No violence, threats, or impermissible or unlawful physical contact.
- No threatening the removal of protections afforded by law.
- Regular monitoring of the interrogation shall be performed by interrogation personnel.

8-69. **False Flag.** (Interrogation) The goal of this technique is to convince the detainee that individuals from a country other than the United States are interrogating him, and trick the detainee into cooperating with US forces. For example, using an interrogator who speaks with a particular accent, making the detainee believe that he is actually talking to representatives from a different country, such as a country that is friendly to the detainee's country or organization. The False Flag approach may be effectively orchestrated with the Fear Down approach and the Pride and Ego Up.

8-70. **Oversight Considerations:** The interrogation chain of command must coordinate an interrogation plan that uses the False Flag approach with the legal representative and the 2X, and receive approval from the first O-6 in the interrogator's chain of command for each specific use of the False Flag approach.

- The use of the False Flag approach must complement the overall interrogation strategy and other approach techniques listed in the interrogation plan.
- When a HUMINT collector intends to pose as a national of a third-party country, that country must be identified in the interrogation plan.
- No implied or explicit threats that non-cooperation will result in harsh interrogation by non-US entities.
- HUMINT collectors will not pose or portray themselves as any person prohibited by this manual, paragraphs 8-10 and 8-11 (for example, an ICRC representative).

8-71. **Separation.** See Appendix M, Restricted Interrogation Technique – Separation.

Selecting an Approach

8-72. There often is insufficient information available to determine an approach other than the direct approach. In this case where the source answers questions but will not discuss pertinent issues, the HUMINT collector may ask direct but nonpertinent questions to obtain sufficient information to develop an approach strategy. This technique is also useful in debriefing to establish rapport. Nonpertinent questions may include—

- Asking about immediate past events. This includes asking an EPW about the circumstances of his capture or asking a refugee about the circumstances concerning his arrival at the refugee point or checkpoint. By doing this, the HUMINT collector can gain insight into the source's current state of mind and, more importantly, he can ascertain his possible approach techniques.
- Asking background questions. This includes asking about the source's family, work, friends, likes, and dislikes. These types of questions can develop rapport and provide clues as to the source's areas of knowledge or reveal possibilities for incentives or emotional approaches.
- Considering what are culturally and socially acceptable topics of discussion. For example, asking an Arab male about his wife could be considered extremely rude, whereas not asking an American the same question might be seen as insensitive.

Making Smooth Transitions

8-73. With the exception of the direct approach, no other approach is effective by itself. HUMINT collectors use different approach techniques or combine them into a cohesive, logical technique. Smooth transitions, sincerity, logic, and conviction are needed to make a strategy work. HUMINT collectors must carefully assess the source's verbal or nonverbal clues to determine when a change in approach strategy is required. The HUMINT collector must guide the conversation smoothly and logically, especially when moving from one approach technique to another. Using transitional phrases can make logical and smooth tie-ins to another approach. By using nonpertinent questions, the HUMINT collector can move the conversation in the desired direction and, as previously stated, sometimes can obtain leads and hints about the source's stresses or weaknesses or other approach strategies that may be more successful.

Recognizing Source Cooperation

8-74. Each source has a point where he will begin to cooperate and answer questions. Some sources will begin answering questions completely and truthfully with no preparation; others might require hours or even days of work. The amount of time that a HUMINT collector spends on an approach depends on a variety of factors. These include—

- The quality and criticality of the information believed to be possessed by the source.
- The presence or absence of other sources that probably possess that information.
- The number of HUMINT collectors and sources available.
- The LTIOV that the HUMINT collector is attempting to obtain.

8-75. The HUMINT collector needs to identify the signs that the source is approaching or has reached the point of cooperation. For example, if during the approach the source leans forward with his facial expression indicating an interest in the proposal or is more hesitant in his argument, he is probably nearing the point where he will cooperate. The HUMINT collector must also be aware of the fact that a source can begin to cooperate in certain areas while continuing to resist strongly in other areas. The HUMINT collector should recognize the reason for refusal, overcome the objection, and stress the benefit of cooperating (reinforce the approach). Once the HUMINT collector determines the source is cooperating, he should interject pertinent questions. If the source does not answer the question, the HUMINT collector should continue with his approach or switch to an alternate approach technique and continue to work until he again believes the source will cooperate. If the source answers the pertinent question, the HUMINT collector continues asking relevant questions until the questioning session is completed.

8-76. If a cooperative source balks at answering a specific line of questions, the HUMINT collector must assess the reason for the refusal. The HUMINT collector may have arrived at a topic that the source finds particularly sensitive. Other reasons that might cause a source to stop answering questions are fatigue or unfamiliarity with the new topic. If this topic is critical, the HUMINT collector may have to reinforce the previously successful approach or may have to use a different approach.

APPROACH STRATEGIES FOR INTERROGATION

8-77. Interrogation does not mean a hostile relationship between the HUMINT collector and the source. In fact, most interrogation sources (90 percent or more) cooperate in response to the direct approach. Unfortunately, those sources who have the placement and access to make them high priority sources are also the ones with the highest degree of security awareness. A source who uses counter-interrogation techniques such as delaying, trying to control the conversation, or interrogating the HUMINT collector himself may—

- Be an intelligence trained soldier.
- Be survival, evasion, resistance, and escape (SERE) trained.
- Be a terrorist.
- Have been a detainee or previously incarcerated.

8-78. In stability and reconstruction operations and civil support operations, detainees are often politically motivated and resistant to most approaches.

8-79. EPWs are normally vulnerable to basic incentive and emotional approach techniques. Most EPWs are traumatized to various degrees by the events preceding or surrounding their capture. They tend to be disoriented and exhibit high degrees of fear and anxiety. This vulnerable state fades over time, and it is vital for HUMINT collectors to interrogate EPWs as soon as and as close to the point of capture as possible. The earlier that an EPW is questioned the more likely he is to cooperate. And the earlier that he begins to cooperate, the more likely he is to continue to cooperate. It is also vital that the HUMINT collector be the first person that the EPW has a chance to talk to. This means that proper silencing and segregation of the sources by whoever is transporting them is an important part of a successful approach.

8-80. The vulnerability of civilian detainees to approach techniques available to the HUMINT collector may be dependent on the exact nature of the conflict. US HUMINT collectors are obligated to treat all detainees in accordance with applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. Detainees and, in particular, EPWs are guaranteed certain rights and privileges. The HUMINT collector may not take any action to remove, state that he will remove, or imply that he will remove any guaranteed right if a detainee fails to cooperate. Under the GPW, EPWs cannot be denied their rights or their privileges accorded them by rank as guaranteed by the GPW. Privileges afforded to them, however, which are not guaranteed by the Geneva Conventions or other applicable law or agreements, may be withheld. (See Appendix A, Section I.) Consult your SJA for questions concerning rights and privileges.

8-81. The HUMINT collector is frequently under a great deal of pressure to "produce results." This situation, coupled with the facts that the HUMINT collector is dealing with threat personnel who may have been attempting to kill US personnel just minutes before questioning and the fact that the source is in a vulnerable state, leads to a tendency to use fear-up techniques. This may, in some circumstances, be the proper approach; however, the HUMINT collector must ensure that in doing so he neither loses control of his own emotions nor uses physical or mental coercion.

APPROACH STRATEGIES FOR DEBRIEFING

8-82. Sources who are debriefed vary even more widely than those who are interrogated. Since debriefing is the systematic questioning of individuals not in the custody of the questioning forces, the HUMINT collector needs to engender an atmosphere of cooperation and mutual benefit. Some sources for debriefing include members of the friendly forces and local personnel. HUMINT collectors often believe that approach techniques are not required for friendly forces and that friendly forces should view debriefing as part of their duties and in their own best interest. However, this is not necessarily the case.

8-83. Many people see debriefing as an interruption in their normal duties and a waste of their time. HUMINT collectors must be sure to stay focused on the purpose and goals of the debriefing. They should be businesslike and must maintain the proper relationship with the source based on his rank and position. The HUMINT collector should allow senior sources more latitude to interpose their opinions and evaluations. A change of scene often facilitates the debriefing of a high-level source since it removes him from his normal distractions, such as the telephone, and allows him to concentrate on the topics being discussed.

8-84. Refugees and DPs are subject to many of the same anxieties and trauma that are experienced by EPWs or other detainees, with the added benefit to the HUMINT collector that they normally have an obvious vested interest in cooperating. Basic incentives usually are sufficient to induce their willing cooperation. The emotional support that can be provided by the HUMINT collector by simply listening and commiserating with their hardship is often sufficient to gain cooperation. The emotional approaches such as love of family and hate toward those who made them refugees are strong motivators toward cooperation.

8-85. The approach techniques used in the questioning of local civilians are probably the most difficult. The approach techniques chosen must take into consideration the attitude of the local population toward the US and its presence and cultural considerations. The local population must see their cooperation as self-beneficial.

APPROACH STRATEGIES FOR ELICITATION

8-86. Elicitation is a sophisticated technique used when conventional collection techniques cannot be used effectively. Of all the collection methods, this one is the least obvious. However, it is important to note that elicitation is a planned, systematic process that requires careful preparation. It is always applied with a specific purpose in mind. This objective is the key factor in determining the subject (which source to question), the elicitor, and the setting. The subject will be selected based on access to or knowledge of the desired information.

8-87. Before approaching the subject, it is necessary to review all available intelligence files and records, personality dossiers, and knowledge possessed by others who have previously dealt with the subject. This will help determine the subject's background, motivation, emotions, and psychological nature. It also may require unobtrusive observation of the subject to establish such things as patterns of activity and likes and dislikes. The setting can be any number of social or official areas. It is important to note that the source should be approached in his natural surroundings, as this will diminish suspicion.

8-88. The key to elicitation is the establishment of a rapport between the elicitor and the source, normally based on shared interests. In the initial stages of an elicitation, the collector confines his conversations to innocuous subjects such as sports and social commentary. Dependent on the value of the source, the collection environment, and the security consciousness of the

source the initial stage could last from a few minutes to numerous seemingly accidental meetings over a period of weeks or months. The HUMINT collector will gradually shift the conversation to topics of collection interest but will be prepared to return to more unthreatening topics based on negative reactions on the part of the subject. Once a topic of interest has been introduced, the HUMINT collector keeps the conversation going by asking for clarification (for example, "I agree, however, what did you mean by….?") or expressing a hypothetical situation.

8-89. There are two basic elicitation approaches: mild flattery and provocation.

- Mild Flattery: Most people like talking about their interests and like talking to those who are knowledgeable and interested in the same topics. People also like to speak to someone who values their opinion on shared interests. The HUMINT collector takes advantage of this. The HUMINT collector leads the conversation into areas that he wishes to collect but does it in such a way that it appears to the source that the source is leading the conversation. Above all in elicitation, the HUMINT collector plays the role of the rapt, attentive, and inquisitive listener.
- Provocation: This is a more dangerous approach and, if used too early in an operation, can alienate the source. Once the HUMINT collector has established shared interests with the source, he can selectively challenge some of the source's statements, encouraging the source to provide more information in support of his view. The HUMINT collector can also insert bits of actual information into the conversation to cause the source to confirm and expound on the topic. Care must be taken so as not to give away more information than is gained.

TERMINATION PHASE

8-90. When it is necessary or prudent, the HUMINT collector will terminate the questioning of a particular source. Whatever the reason for terminating, the HUMINT collector must remember there is a possibility that someone may want to question the source at a later date. There are many reasons why a HUMINT collector may want or need to terminate questioning:

- The source remains uncooperative during the approach phase.
- The collection objective cannot be met in one questioning session.
- The HUMINT collector fails to maintain rapport and loses control of the questioning.
- The collection objectives have been satisfied.
- The HUMINT collector or the source becomes physically or mentally unable to continue.
- Information possessed by the source is of such value that his immediate evacuation to the next echelon is required.
- The HUMINT collector's presence is required elsewhere.

8-91. There are many ways to conduct a termination, but the following points must be conveyed to the source:

- The HUMINT collector should sincerely and convincingly reinforce successful approaches. All promised incentives should be rendered.
- The source must be told the information he gave will be checked for truthfulness and accuracy. His reaction to this statement should be closely monitored. The exact form of this statement will be dependent on the situation. It should not be done in a manner to alienate a cooperative source.
- The source must be told that the same or another individual may speak to him again. This sets the stage for future contacts.
- Any identification must be returned to the source. If the HUMINT collector has other documents or belongings of the detainee (such as letters or photographs), he will either return them to the detainee, if appropriate, or will turn them over to the MP guard. Depending on the circumstances and the legal status of the detainee, the MPs will retain the detainee's property and return the property to him at the end of his internment.
- In a debriefing, the HUMINT collector will normally ask the source not to discuss the subject of the questioning for his own protection. In interrogation operations, the HUMINT collector normally coordinates with the holding area guards to have the detainees who have been interrogated kept separate from sources who have not yet been interrogated if the situation allows.

Chapter 9

Questioning

9-1. Questioning is one of the five phases of HUMINT collection. Developing and using good questioning techniques enable the HUMINT collector to obtain accurate and pertinent information and to extract the maximum amount of information in the minimum amount of time. The HUMINT collector must know when to use different types of questions.

GENERAL QUESTIONING PRINCIPLES

9-2. Questions should be presented in a logical sequence to avoid neglecting significant topics. The HUMINT collector begins the questioning phase with the first topic in the sequence he tentatively established as part of his questioning plan. He obtains all of the source's pertinent knowledge in this topical area before moving on to the next topic in his sequence. The only exception is exploiting a hot lead, which is discussed in paragraph 9-21.

9-3. The HUMINT collector must at all times remember that his mission is the rapid collection and dissemination of accurate information. He must not allow himself to be sidetracked into nonpertinent discussions or debates nor should he express distaste or value judgments on the information being supplied unless that is a planned part of his approach technique. The HUMINT collector uses vocabulary that is clear, unambiguous, and understandable by the source. The source may not be on the same intellectual level or have the same degree of education as the HUMINT collector, so the HUMINT collector must adapt his questioning to the level of the source. The source may also have specific technical knowledge, more education and/or a higher intellectual level than the HUMINT collector. In this case, the HUMINT collector normally relies on prepared questions or technical support for his questioning. Without good systematic questioning techniques, even the most cooperative source may provide only minimal usable information.

DIRECT QUESTIONS

9-4. Direct questions are basic questions normally beginning with an interrogative (who, what, where, when, how, or why) and requiring a narrative answer. They are brief, precise, and simply worded to avoid confusion. The HUMINT collector must consider the probable response of the source to a particular question or line of questioning and should not, if at all possible, ask direct questions likely to evoke a refusal to answer or to antagonize the source.

TYPES OF DIRECT QUESTIONS

9-5. The HUMINT collector must be able to use the following types of direct questions:

- Initial, topical.
- Follow-up.
- Nonpertinent.
- Repeat.
- Control.
- Prepared.

Initial Questions

9-6. The HUMINT collector begins his questioning with the first topic in his collection plan and asks all the basic questions necessary to cover the topic. The answers to the basic questions will determine the requirements for follow-up questioning. The initial questions are directed toward obtaining the basic information on the topic. In other words, they are the "who, what, where, when, how, and why" of each topic.

Follow-up Questions

9-7. Follow-up questions are used to expand on and complete the information obtained from the initial questions. Often even if the initial question is a well-constructed direct question, it will elicit only a partial answer. For example, when asked, "Who is going to attack?" The source might say, "My unit." Follow-up questions are used to determine precisely what the source means by "my unit" and what other units may also attack. The answer to follow-up questions may lead to more follow-ups until the source's knowledge on a given topic is exhausted. At a minimum, upon receiving a positive answer to an initial question, the HUMINT collector needs to ask "Who (what, where, when, why, how) else?" For example, if the HUMINT collector asks the source, "Who, in the local government is collaborating with the insurgents?" and is told a name in response, he will ask follow-up questions to determine all the required information about this individual and then will ask, "Who else, in the local government is collaborating with the insurgents?" This will continue until the source's knowledge in this area is exhausted.

Nonpertinent Questions

9-8. Nonpertinent questions are questions that do not pertain to the collection objectives. They are used to conceal the collection objectives or to strengthen rapport with the source. They are essential when the collector is using the elicitation technique. Nonpertinent questions may be used to gain time for the HUMINT collector to formulate pertinent questions and may also be used to break the source's concentration, particularly, if the HUMINT collector suspects the source is lying. It is hard for a source to be a convincing liar if his concentration is frequently interrupted.

Repeat Questions

9-9. Repeat questions ask the source for the same information obtained in response to earlier questions. They are a method to confirm accuracy of important details such as place names, dates, and component parts of technical equipment and to test truthfulness. Repeat questions should not be exact repetitions of an earlier question. The HUMINT collector must rephrase or otherwise disguise the previous question. The repeat question also needs to be separated in time from the original question so that the source cannot easily remember what he said. Repeat questions may also be used to develop a topic the source had refused to talk about earlier.

Control Questions

9-10. Control questions are developed from recently confirmed information from other sources that is not likely to have changed. They are used to check the truthfulness of the source's responses and should be mixed in with other questions throughout the questioning. If a source fails to answer a control question as expected, it may be an indicator that he is lying. However, there are other possible explanations. The source—

- Could have misunderstood the question.
- Could be making up information in order to please the questioner and/or receive a promised incentive.
- Could have answered the question truthfully to the best of his ability, but his information could be wrong or outdated.
- May be correct and the information that the control question was based on is no longer true.

9-11. It is the responsibility of the HUMINT collector to determine, through follow-up questions, which of the possibilities is the case. The HUMINT collector should also consult with the HAT for assistance in verifying the source reporting through all-source analysis.

Prepared Questions

9-12. Prepared questions are questions developed by the HUMINT collector, normally in writing, prior to the questioning. Prepared questions are used primarily when dealing with information of a technical nature or specific topic, which requires the HUMINT collector to formulate precise and detailed questions beforehand. The HUMINT collector may have to research analytical or technical material or contact SMEs to assist him in preparing questions. HUMINT collectors must not allow the use of prepared questions or any limitations to their education or training to restrict the scope and flexibility of their questioning. In many instances, the HUMINT collector should have an analyst or technical expert “sit in” on the questioning as well.

9-13. The HUMINT collector must be able to use the different types of questions effectively. Active listening and maximum eye-to-eye contact with the source will provide excellent indicators for when to use follow-up, repeat, control, and nonpertinent questions. The HUMINT collector must use direct and follow-up questions to fully exploit subjects pertinent to his interrogation objectives. He should periodically include control, repeat, and nonpertinent

questions in order to check the truthfulness and consistency of the source's responses and to strengthen rapport.

TYPES OF QUESTIONS TO AVOID

9-14. When using the questioning methodologies of interrogation, HUMINT collectors should avoid using negative, compound, or vague questions. Leading questions are usually to be avoided, but some special questioning techniques, such as use of a polygraph, require the use of leading questions.

Leading Questions

9-15. Leading questions are questions that are constructed so as to require a yes or no answer rather than a narrative response. They generally begin with a form of the verb "to be" (such as "is," "was," "were," "will," "are"). For example, "Is the mayor working with the insurgents?" Leading questions should generally be avoided for the following reasons:

- They make it easier for the source to lie since the source only provides minimal information.
- It takes longer to acquire information.
- A source, particularly one that is frightened or trying to get an incentive, will tend to answer in the way that he thinks the HUMINT collector wants him to answer.

9-16. Although normally avoided during questioning, an experienced HUMINT collector may use leading questions when the technical nature of the subject matter or the specific information needed leaves no alternatives. Leading questions can be used to—

- Verify specific facts.
- Pinpoint map locations.
- Confirm information obtained during map tracking.
- Transition from one topic area to another.

Negative Questions

9-17. Negative questions are questions that contain a negative word in the question itself such as, "Didn't you go to the pick-up point?" If the source says "yes," the HUMINT collector is faced with the question of whether he means "yes, I went to the pick-up point" or "yes, I didn't go to the pick-up point." When the source answers, the HUMINT collector cannot be sure what the answer means; therefore, he must ask additional questions. This can be particularly confusing when working with an interpreter. Other cultures may interpret a negative question in a way other than what the HUMINT collector meant. Negative questions should never be used during questioning unless they are being used deliberately during the approach to make the source appear to contradict himself. In other instances, the insertion of negative words within the question makes them impossibly open-ended. For example, "Who didn't attend the meeting?"

Compound Questions

9-18. Compound questions consist of two questions asked at the same time; for example, "Before you were captured today, were you traveling north or south?" Or “Where were you going after work and who were you to meet there?” They are easily misunderstood and may confuse the source or force him to give an ambiguous answer. Compound questions allow the source to evade a part of the question or to give an incomplete answer.

Vague Questions

9-19. Vague questions do not have enough information for the source to understand exactly what the HUMINT collector is asking. They may be incomplete, general, or otherwise nonspecific and create doubt in the source's mind. Vague questions confuse the source, waste time, and are easily evaded. They result in answers that may confuse or mislead the HUMINT collector and require further follow-up questions.

ELICITATION

9-20. Elicitation is the gaining of information through direct interaction with a human source where the source is not aware of the specific purpose for the conversation. Elicitation is a sophisticated technique used when conventional questioning techniques cannot be used effectively. Of all the collection methods, this one is the least obvious. However, it is important to note that elicitation is a planned, systematic process that requires careful preparation. Elicitation is always applied with a specific objective in mind and normally directed toward a specific source.

LEADS

9-20. A lead is a statement made by a source spontaneously or in response to questioning that leads the questioner to believe that the source has information on a topic other than the one currently under discussion. Documents captured with or on the source may also be exploited as sources of leads. Leads are referred to as either “hot” or “cold.”

HOT LEADS

9-21. A hot lead is a statement made by a source either spontaneously or in response to questioning that indicates he has information that could answer intelligence requirements on a topic other than the one currently under discussion. The lead could also be on a topic that although not listed as a requirement is, based on the HUMINT collector’s experience, of critical importance. Information on WMD and information on US personnel being held by threat forces are normally considered hot leads even if not listed as requirements. The HUMINT collector will normally question the source immediately on a hot lead, unless he is already asking questions on another topic. In this case, he completes questioning and reports the information on the priority topic, as appropriate, and then immediately questions on the hot lead. As soon as the HUMINT collector is sure he has obtained and recorded all the details known to the source, he reports the hot lead information by the

most expedient means available, normally in SALUTE report format. The HUMINT collector then resumes his questioning of the source at the point where the hot lead was obtained.

COLD LEADS

9-22. A cold lead is a statement made by a source either spontaneously or in response to questioning that indicates he has information on a topic of interest other than the one currently under discussion but that would not answer PIRs. The HUMINT collector makes note of the cold lead and exploits it after the planned questioning objectives have been satisfied or at the appropriate time during the questioning sequence.

DETECTING DECEIT

9-23. HUMINT information often has the capability to be more accurate and reliable than other disciplines. SIGINT information, for example, is not always able to return to the original source of the information to determine the reliability of the information, and interpretation of IMINT information may be uncertain. However, while HUMINT can be reviewed for reliability, determining the reliability of human sources is a continuous process accomplished by carefully assessing not only the sources of information but also assessing the information itself.

9-24. Detection of deception is not a simple process, and it normally takes years of experience before a HUMINT collector can readily identify deliberate deceit. Inconsistencies in the source's actions or words do not necessarily indicate a lie, just as consistency is not necessarily a guarantee of the truth. However, a pattern of inconsistencies or unexplainable inconsistencies normally indicate deceit.

TECHNIQUES FOR IDENTIFYING DECEIT

9-25. Techniques for identifying deceit include but are not limited to the following:

- Repeat and control questions (see paras 9-9 and 9-10).
- Internal inconsistencies. Frequently when a source is lying, the HUMINT collector will be able to identify inconsistencies in the timeline, the circumstances surrounding key events, or other areas within the questioning. For example, the source may spend a long time explaining something that took a short time to happen, or a short time telling of an event that took a relatively long time to happen. These internal inconsistencies often indicate deception.
- Body language does not match verbal message. An extreme example of this would be the source relating a harrowing experience while sitting back in a relaxed position. The HUMINT collector must be careful in using this clue since body language is culturally dependent. Failing to make eye contact in the US is considered a sign of deceit while in some Asian countries it is considered polite.
- Knowledge does not match duty position or access. Based on the source's job, duty position, or access the HUMINT collector should have

developed a basic idea of the type and degree of information that an individual source should know. When the source's answers show that he does not have the expected level of information (too much or too little or different information than expected), this may be an indicator of deceit. The HUMINT collector needs to determine the source of unexpected information.

- Information is self-serving. Reporting of information that is self-serving to an individual or his group should be suspect. For example, a member of one ethnic group reporting generic atrocities by an opposing ethnic group or a source reporting exactly the right information needed to receive a promised incentive should be suspect. That is not to say that the information is necessarily false, just that the HUMINT collector needs to be sure to verify the information.
- Lack of extraneous detail. Often false information will lack the detail of truthful information, especially when the lie is spontaneous. The HUMINT collector needs to ask follow-up questions to obtain the detail. When the source is unable to provide the details that they should know, it is an indicator of deceit. If the source does provide this additional information, it needs to be checked for internal inconsistencies and verified by repeat questions.
- Repeated answers with exact wording and details. Often if a source plans on lying about a topic, he will memorize what he is going to say. If the source always relates an incident using exactly the same wording or answers repeat questions identically (word for word) to the original question, it may be an indicator of deceit. In an extreme case, if the source is interrupted in the middle of a statement on a given topic, he will have to start at the beginning in order to "get his story straight."
- Source appearance does not match story. If the source's physical appearance does not match his story, it may be an indication of deceit. Examples of this include the source who says he is a farmer but lacks calluses on his hands or the supposed private who has a tailored uniform.
- Source's language usage does not match story**.** If the type of language, including sentence structure and vocabulary, does not match the source's story, this may be an indicator of deceit. Examples of this include a farmer using university level language or a civilian using military slang.
- Lack of technical vocabulary. Every occupation has its own jargon and technical vocabulary. If the source does not use the proper technical vocabulary to match his story, this may be an indictor of deceit. The HUMINT collector may require the support of an analyst or technical expert to identify this type of deceit.
- Physical cues. The source may display physical signs of nervousness such as sweating or nervous movement. These signs may be indicators of deceit. The fact that an individual is being questioned may in itself be cause for some individuals to display nervousness. The HUMINT collector must be able to distinguish between this type of activity and nervous activity related to a particular topic. Physical reaction to a

particular topic may simply indicate a strong emotional response rather than lying, but it should key the HUMINT collector to look for other indicators of deceit.

- Failure to answer the question asked. When a source wishes to evade a topic, he will often provide an answer that is evasive and not in response to the question asked. For example, if the source is asked, "Are you a member of the insurgent organization?" and he replies, "I support the opposition party in the legislature," he has truthfully answered a question, but not the question that was asked. This is a subtle form of deceit since the source is seemingly cooperative but is in fact evading providing complete answers.

ACTIONS UPON IDENTIFYING INDICATORS OF DECEIT

9-26. The exact actions by the HUMINT collector when identifying possible deceit are dependent on the type of collection, the circumstances of the collection, the specific sign of deceit observed, the type of approach used, and cultural factors. The HUMINT collector may—

- Question the topic in more detail looking for additional indicators.
- Reinforce the approach.
- Move to another topic and revisit the original topic later with repeat questions. Ask control questions (confirmed by known data) and questions to which the source should know the answer to see if he answers honestly.
- Point out the inconsistency to the source and ask for an explanation.
- Seek assistance from a more experienced HUMINT collector, analyst, or a technical expert on the culture or the topic being questioned.
- Conduct continuous assessments of source (see FM 34-5 (S//NF)).
- Research established databases.
- Ask yourself if the information makes sense; if not, conduct more research.
- Consider how the information was obtained.
- Compare the information provided to the source's placement and access.
- Compare answers with other sources with similar placement and access. Be aware that this method is merely a rough tool to check veracity and should not be used by the collector to confirm intelligence.
- Use the polygraph.
- Consider that a source motivated primarily by money will likely be tempted to fabricate information in order to get paid.
- Be aware that a source may read the local newspaper to report information that is already known or may also be providing information to another agency.

9-27. The one thing that the HUMINT collector cannot do is to ignore signs of deceit.

HUMINT COLLECTION AIDS

9-28. There are numerous procedural and recording aids that can assist the HUMINT collector in conducting rapid, accurate, yet systematic questioning. They include—

- HUMINT Collector's Guide. This guide is a pamphlet or notebook designed to guide the HUMINT collector through the questioning. The HUMINT team leader should ensure that team members prepare a HUMINT collector's guide, which could be included in the unit's SOP. The guide is made based on the AO and supported command intelligence requirements. The HUMINT collector and available intelligence analysts should jointly prepare the guide. Appendix G provides the basic topics and example questions that can be adapted to construct a HUMINT collector's guide. The guide must be updated for each interrogation as part of planning and preparation. The guide should contain information such as—
 - Intelligence requirements and ISR tasks.
 - Topical questioning sequence format.
 - Actual prepared questions to be used during questioning.
 - Guidelines for employing the various approach techniques.
 - Formats or samples of completed reports used by HUMINT collectors.
- Time Event Chart. A timeline, or event chart, is a graphic display upon which the HUMINT collector enters chronological information as it is collected. This facilitates the HUMINT collector in understanding and organizing the collected information. It also enables the HUMINT collector to identify gaps in information, to sequence events properly to facilitate follow-up questions, and to identify deception. The HUMINT collector can develop a basic timeline prior to questioning. The source should not be able to observe the timeline since doing so will help a deceptive source "keep his story straight." See Chapter 12 for how to create and use a time event chart.
- Organizational Chart. An organizational chart is a graphic representation of an organization. It is the equivalent of a military line-and-block chart. This is used to facilitate the questioning of organizations and in establishing their hierarchical and lateral linkages. A basic chart can be developed prior to the questioning based on the expected organizational questioning.

RECORDING TECHNIQUES

9-29. Accuracy and completeness are vital principles to reporting. However, it is usually not possible to completely record all information in a questioning session. Recording techniques may involve memory, handwritten or typed notes, tape recordings, and video recordings. Each has its advantage and corresponding disadvantage.

- Memory: Relying on one's memory has certain advantages. It does not require any equipment or extra time, and is the least intrusive method of recording information. It allows maximum interaction with the source and projects sincerity. An individual can train himself to

remember highly detailed information. Often in elicitation, memory is the only viable recording method. However, in general, using the memory exclusively to record information is the most inaccurate methodology. Particularly in a long questioning session, details are forgotten and information tends to be generalized.

- Handwritten notes: Handwritten notes require minimal equipment (a pad and pencil), are not intimidating to most sources, and can be as detailed as the HUMINT collector desires. If an analyst or second interrogator is present, he should also take notes. This second set of notes can aid in report writing. The interrogator should not rely solely on an analyst's notes unless absolutely necessary. However, writing notes while questioning an individual often interferes with the rapport between the collector and the source. The collector loses eye contact and can easily miss subtle body language that might indicate lying. Detailed note taking can be extremely time consuming and many sources will, over time, begin to limit their responses so they do not have to repeat information or wait for the collector to write it down. It is somewhat intrusive and inhibiting to the source and is totally inappropriate in certain situations such as liaison and most casual source contacts. Handwritten notes can also be inaccurate, have limited details, and can be hard to read after the fact.
- Computer notes: With the proliferation of computer equipment, particularly laptops and handheld devices, note taking on computers is increasingly commonplace. A computer can provide access to data-based information that may support questioning such as foreign language dictionaries or technical support manuals, either through the Internet (if connected) or on its harddrive. If the computer is linked to a communications system, it also allows the HUMINT collector to transmit data, including SALUTE reports, during the course of the questioning. Notes taken on a computer, however, have many of the same disadvantages as handwritten notes. In addition, computer notetaking requires more equipment and technological support and access to either electricity or a plentiful supply of batteries. Computers may be intimidating to some sources and the fact that what the source says is being entered into a computer may cause the source to alter the information he is providing. Computers tend to isolate the collector from the source by dividing the collector's attention between the computer and the source, and again may cause the collector to miss critical body language clues. Finally, the computer is even more inappropriate to casual and controlled source operations than are handwritten notes.
- Audiotapes: If recording equipment is discrete and functioning properly, audiotapes can be extremely accurate. Use of tapes also allows the HUMINT collector to place his entire attention on the source. This not only enhances rapport but also allows the HUMINT collector to observe the source's body language. Taping a questioning session, if done overtly though, tends to be extremely inhibiting to the source and may seriously curtail the information obtained. Surreptitious taping can be illegal in some situations and dangerous in some situations as well. Consult your legal advisor to determine if

taping is legal. Taped information can also be seriously affected by ambient noise and the relative positioning of the source and collector to the microphone. Writing a report based on a taped session can be extremely time consuming, since it takes as long to listen to a tape as it took to record it. This drawback can be reduced somewhat through the use of voice activated recording devices. Exclusive dependence on audiotapes tends to make the collector less attentive and more likely to miss follow-up questions. Also, if the tape is lost or damaged or does not function properly, the collector has no backup.

- Video recording: Video recording is possibly the most accurate method of recording a questioning session since it records not only the voices but also can be examined for details of body language and source and collector interaction. It is also the most resource intensive requiring proper lighting, cameras, viewing equipment, and possibly trained operators. If done overtly, video recording can be by far the most inhibiting to the source. Even if the source is willing to be videotaped, there is a tendency for both the source and the collector to "play to the camera," creating an artificiality to the questioning. Consult your legal advisor to determine the legality of overt or covert videotaping.

QUESTIONING WITH AN ANALYST OR A TECHNICAL EXPERT

9-30. The HUMINT collector may often find himself in the position where he needs to use an analyst or a technical expert, or both, in order to conduct questioning. Many of the techniques involved in using an analyst or technical expert are the same as those with using an interpreter (see Chapter 11). The HUMINT collector must pre-brief these supporting personnel. The degree to which the analyst or technical expert is involved in the actual questioning is dependent on the established relationship between the analyst or technical expert and the HUMINT collector. The HUMINT collector will always remain in charge of the questioning, be present throughout the questioning, and ensure that the questioning follows his questioning plan. He must ensure that the supporting analyst or technical expert has the proper security clearance.

9-31. An analyst or technical expert can participate in the questioning to various degrees listed below from least intrusive to most intrusive. As the degree of participation by the analyst or technical expert increases, the technical fidelity of the information collected usually increases but the rapport between the HUMINT collector and the source decreases as does the HUMINT collector's ability to control the content and judge the truthfulness of the information. The analyst or technical expert may provide—

- Advice Only: The HUMINT collector does the questioning. The expert provides information prior to the meeting and may review the collected information after the meeting. The technical expert is not present at the actual questioning.
- Remote Support: The HUMINT collector does the questioning. In addition to the above, the expert monitors the questioning and provides input to the HUMINT collector after the questioning as required. Based on the technological support, this can involve the expert sitting in on, but not participating in the questioning (which

may make the source uncomfortable), or the expert viewing and listening to the questioning through a remote video and sound hook-up.

- Local Support: The HUMINT collector does the questioning. The expert sits in on the questioning and provides input to the HUMINT collector during the course of the questioning. This can break both the source's and the HUMINT collector's trains of thought and confuse the lines of control in the questioning.
- Expert Participation: The HUMINT collector initiates the questioning, but the expert participates throughout the questioning, asking for clarification and additional information as required. Unless properly trained, the expert can seriously taint the quality of the information through the use of poor questioning techniques. The HUMINT collector can lose rapport and control.
- Trained Expert Questioning: In rare instances, with particularly difficult technical topics or those areas of questioning that require a high degree of technical expertise, it may be easier to train the expert in basic questioning techniques than it is to train the HUMINT collector on the technical topic. In this instance, the HUMINT collector sits in on the questioning to ensure proper procedures and techniques are used and to advise the technical expert. The technical expert does most of the questioning.

9-32. In any case, if the source is to receive compensation for his time, it must come from the HUMINT collector, not the analyst or technical expert. This continues to reinforce that the HUMINT collector is in charge, and does not transfer the source's trust to the expert.

THIRD-PARTY OFFICIAL AND HEARSAY INFORMATION

9-33. The source may have information that he did not observe firsthand. While this information is not as reliable as firsthand knowledge, it is often significant enough to report. The HUMINT collector must be careful to identify this information as to its origin, type, and the time and manner that the information was obtained by the source. This information will be entered into the report as a source comment or a collector comment. This will include—

- The origin of the information. This may be the name, rank, and duty position or job of an individual or may be an official or unofficial document such as an OPORD, official memorandum, or party newspaper.
- The complete organization to which the person who provided the information belongs or the identity of the organization that produced the official or unofficial document from which the source obtained the information.
- Date-time group (DTG) when the source obtained the information.
- The circumstances under which the source obtained the information.

9-34. Comparing the details of the hearsay information, such as DTG, where the information was obtained and the circumstances under which the source

claimed to have received it, to the source's known activities, may provide indications of truthfulness or deception on the part of the source.

CONDUCTING MAP TRACKING

9-35. Map tracking is a specific questioning skill that the HUMINT collector uses in all operations. It is a vital skill in supporting targeting and operational planning. Map tracking identifies and verifies key information by tracking the source's movement and activities within a specific area over a fixed period using a map or similar graphic aid. The area and the time involved are dependent on the collection requirements and the source's knowledge level. Map tracking can occur at any point in the questioning process. Normally, the HUMINT collector begins map tracking as soon as his questioning identifies a priority disposition or activity that the source's information can locate on the map.

9-36. Map-tracking techniques, if properly applied, can extract information from friendly, neutral, or threat sources and can be used with individuals ranging from those with detailed map skills to illiterates, and those who have never seen a map. Through map tracking, the HUMINT collector pinpoints locations of any threat activity, threat dispositions, or any other priority terrain-related information, such as trafficability, known to the source.

9-37. The HUMINT collector will determine these locations with the degree of fidelity needed to support operational requirements. The degree of detail needed may range from an 8-digit grid coordinate for unit locations to locations of specific buildings, rooms, or even items within a room. The HUMINT collector uses a variety of map-tracking aids including standard military maps, aerial photographs, commercial imagery, building blueprints and diagrams, and commercial road maps. Some advantages to map-tracking techniques include—

- The source is led through his memory in a logical manner.
- Discrepancies in the source's statements are easier to detect.
- Locations are identified to support targeting and battlefield visualization.
- Map tracking is a four-step process:
 - Step 1: Determine the source's map-reading skills.
 - Step 2: Establish and exploit common points of reference (CPRs).
 - Step 3: Establish routes of travel.
 - Step 4: Identify and exploit key dispositions.

DETERMINE THE SOURCE'S MAP-READING SKILLS

9-38. The first step in the map-tracking process is to determine the specific map-reading skills of the source. This step only occurs the first time that the HUMINT collector map tracks a particular source. This information will determine what methodology will be used for the rest of the process. In this step the HUMINT collector is determining existing skills; he should not attempt to teach the source additional map skills at this time. The HUMINT collector can use prior knowledge, such as the fact that the source is illiterate or cannot read a map, to skip some of the specific parts of the process. Below

is a detailed description of the process to establish the map-reading skills of the source.

- The HUMINT collector asks the source if he can read the map being used. If the source answers in the affirmative, the HUMINT collector asks some key questions to verify this.
- If the source cannot read the map being used, the HUMINT collector determines if the source can read another type of available map or graphic representation. For example, a source may not be able to read a military map but might be able to use a commercial map or an imagery product.
- The HUMINT collector then establishes the method that will be used to describe movement (direction and distance) on the map. If the source knows how to use compass directions, that may be the most expedient method for determining direction. Again, the HUMINT collector must verify that the source knows how to use compass directions. This can be done best by having the source tell the compass directions between known points. Distance is normally determined by using the standard units of measurement with which the source is familiar, such as kilometers or miles. This can cause some problems, for example, if the map is measured in kilometers and the source normally expresses distance in miles. The HUMINT collector must make the adjustment rather than trying to teach the source the unfamiliar system.
- Compass directions and standard units of measure are not the only method or necessarily even the best method of indicating direction and distance in all circumstances. When using an urban map, direction and distance can often be described by indicating blocks traveled and turns made (right or left) at intersections. Direction of travel can be indicated in reference to key features such as going toward the downtown area or moving toward the river. When describing the interior of a building, references may be to upstairs, downstairs, floor number, or other descriptive terms. When map tracking in rural areas, especially when questioning someone who does not know how to use compass directions, terrain association is normally the best method of establishing direction of travel and distance. Questions such as "Were you traveling uphill at that time?" "What prominent terrain features could you see from that location?" "What was the nearest town?" or "Was the sun behind you?" help to identify locations on the map. The HUMINT collector should allow the source to use his own frames of reference. However, the HUMINT collector must ensure he understands the source.

ESTABLISH AND EXPLOIT COMMON POINTS OF REFERENCE

9-39. The second step of map tracking is to establish CPRs. It is important in accurate map tracking to talk the source through his past activities in the sequence in which they occurred and his movements in the direction in which they were traveled. Attempting to track a source backward in time and space is time consuming, inaccurate, and is often confusing to both the source and the HUMINT collector. Future activities should be tracked in the direction in

which they are planned to occur. The HUMINT collector will normally establish various CPRs throughout the questioning of the source.

9-40. For certain sources such as friendly forces, tasked sources, or other instances where the starting and ending points of the mission being questioned are easily established, the first point of reference is normally where that source began the mission. For other sources such as detainees, line crossers, informers, and refugees, it is often more difficult to establish a "starting point." In these instances the HUMINT collector uses a sequential approach to the map tracking. He establishes a point of reference that is a logical end point for the subject being discussed. This may be, for example, the point of capture for a detainee, the point where a line crosser entered the friendly force area, or where a refugee left the area of intelligence interest. Second and subsequent points of reference are established during questioning when the source mentions a disposition, activity, or location of interest that can be located on the map. The HUMINT collector locates the reference point on the map through direct questioning and terrain association. He uses leading questions as necessary to establish an exact location. He then establishes the route of travel.

ESTABLISH ROUTES OF TRAVEL

9-41. Once the CPR is established, the HUMINT collector questions the source until he has extracted all pertinent information on the CPR and its immediate surroundings. For past missions and activities, the HUMINT collector then establishes the route the source traveled between the newly established CPR and a previously established CPR and exploits the route. For future missions or activities, the route is established from the previously established CPR toward the future mission CPR.

9-42. The HUMINT collector should establish the route traveled by determining the source's direction and physical description of the route of travel. The description should include details such as surface on which the source traveled and prominent terrain features along the route of travel and the distance the source traveled or, in the case of future locations, would travel. The HUMINT collector should also identify any pertinent dispositions or any activities of military significance, belonging to the opposition forces, along or in the vicinity of the route of travel. For longer routes, the HUMINT collector may divide the route into segments for ease of questioning.

IDENTIFY AND EXPLOIT KEY DISPOSITIONS

9-43. The HUMINT collector must obtain the exact location and description of every pertinent disposition known to the source. This includes the locations established as CPRs and any other pertinent disposition established during map tracking. At a minimum, the collector should—

- Establish a physical description of the disposition. The degree of fidelity will depend on the collection requirements. This may be as detailed as the physical layout of a room to the general description of a training area. This will include security measures and modus operandi at the location as appropriate.

- Identify and describe the significance of the disposition in terms of ongoing and future threat operations.
- Identify and describe key activities, equipment, or organizations at the location, as well as people and leaders.
- Identify and describe all pertinent collocated activities, locations, or organizations, as well as people and leaders.
- Identify the basis (hearsay or personal experience) and DTG of the source's knowledge of each disposition.

SPECIAL SOURCE CATEGORIES

9-44. Questioning of every source is unique and requires specific preparation. Special consideration and preparation must be made for some specific categories of sources. Some examples of special source categories include but are not limited to wounded or injured sources or illiterates.

WOUNDED OR INJURED SOURCES

9-45. HUMINT collectors may question (interrogate, debrief, or elicit information from) a wounded or injured source provided that they obtain certification from a competent medical authority that the questioning will not delay or hinder medical treatment or cause a worsening of the condition of the source. The HUMINT collector can question the source before, after, or during medical treatment. The HUMINT collector cannot at any time represent himself as being a doctor or any other type of medical personnel or member of the ICRC. Nor can he state, imply, or otherwise give the impression that any type of medical treatment is conditional on the source's cooperation in answering questions.

ILLITERATES

9-46. HUMINT collectors should never make the mistake of equating illiteracy with a lack of intelligence or an inability to provide meaningful information. In fact, many illiterates have developed extremely good memories to compensate for their inability to rely on the written word. An illiterate's frame of reference does not include street signs, mile markers, and calendars. It also will probably not include conventional time and distance measurements. The HUMINT collector must compensate for these differences. Map tracking, for example, must normally be accomplished by terrain association. If the source cannot tell time, time of day can be determined by the position of the sun.

Chapter 10

Reporting

10-1. Reporting is the final and in many cases the most vital phase in HUMINT collection. If the collected information is not reported accurately, in a timely manner, in the proper format, and to the correct recipient, it cannot become part of the all-source intelligence product or tip in time to affect operational decisions. Information that would support targeting must be reported by the fastest means possible.

REPORTING PRINCIPLES

10-2. The HUMINT collector must be able, in a written report, to convey to the user the information obtained from a source. Therefore, the following principles of good report writing are to be followed:

- Accuracy. Accurately reflect the information obtained from the source. Reporter comments and conclusions must be clearly identified as such.
- Brevity. Report all relevant information; however, the report should be brief, to the point, and avoid unnecessary words.
- Clarity. Use simple sentences and understandable language. Proper grammar and punctuation are a must. Another team member, if possible, should read the reports to ensure clarity.
- Coherence. Present the information in a logical pattern based on standard reporting formats.
- Completeness. Report all information collected. The collector should not filter information since all information is of interest to an analyst. Report negative responses to pertinent topics to prevent a misunderstanding or duplication of effort in subsequent questioning based on SDRs.
- Timeliness. Report information as soon as operationally feasible. Most collection requirements contain a LTIOV as part of the requirement. While written reports are preferable, critical or time-sensitive information is passed by the most expedient means available.
- Releasability. Include only releasable information in reports that are to be shared with multinational units. When possible, reports to be shared with multinational units should be kept to the appropriate classification to ensure the widest dissemination of the reported information.

REPORT TYPES

10-3. There are two major categories for reporting information: operational reports and source administrative reports. Figure 10-1 shows the HUMINT

reporting channels. Refer to DIAM 58-11 (S//NF) and DIAM 58-12 (S//NF) for specific guidance in using these reports.

OPERATIONAL REPORTS

10-4. Operational reports is a broad category that encompasses all reports that do not contain information collected in response to intelligence requirements or the reporting of the technical, and usually sensitive, aspects of HUMINT collection. It includes but is not limited to all administrative and logistical reports. Unit SOPs and directives from higher headquarters establish operational reporting requirements, formats, and procedures. Operational reporting—

- Tells the commander where and when assets are conducting missions.
- Describes unit mission capability.
- Responds to administrative and logistical requirements.
- Describes support requirements.
- Includes but is not limited to unit status reports, mission planning reports, mission status reports, and equipment status.
- Reports ICF usage at any echelon where the use of ICFs is authorized.

SOURCE ADMINISTRATIVE REPORTS

10-5. Source administrative reports include intelligence reports that are used to pass or request information in order to answer intelligence requirements, and reports that address the HUMINT collector's contacts with the source. Intelligence reports include but are not limited to IIRs and SALUTE reports.

Intelligence Information Reports

10-6. The IIR is used to report all HUMINT information in response to collection requirements. It is used to expand on information previously reported by a SALUTE report or to report information that is either too extensive or not critical enough for SALUTE reporting. IIRs are written at any echelon and "released" by the appropriate authority before they enter the general Intelligence Community. Normally the G2X will be the release authority for IIRs.

10-7. At the tactical level, the HUMINT collectors will fill out the complete IIR; however, the requirements section may link the information collected against a unit requirement rather than against national requirements. In any case, the report will be forwarded to the OMT.

10-8. The team leader will review the IIR, place a copy of the IIR in the detainee's or source's local file and forward the IIR to the OMT. (When a detainee is transferred to another facility or evacuated to a higher echelon, a copy of each IIR written from interrogations of that detainee is forwarded with him.) The OMT reviews the report, requests additional information as necessary from the originator, adds additional administrative detail, and forwards the report to the HOC of the supporting C/J/G/S2X. The HOC and the 2X review the report, request additional information as required, add any

final required information including linking it to national requirements, and then the 2X releases the report.

10-9. In addition to the above, the text information from the IIR can be forwarded to the unit's analytical elements and when it contains critical time-sensitive information, such as an impending attack, it is sent to units which may be affected by the information; however, it must be clearly marked "unevaluated information, not finally evaluated intelligence." The use of IIRs and the formats are covered in DIAM 58-12 (S//NF).

SALUTE Reports

10-10. The SALUTE report is a standard Army format used to report information of immediate interest by individuals at any echelon. (See Appendix H for a SALUTE report format.) The SALUTE report is the primary means used to report combat information to units that could be affected by that information. After review by the team leader, SALUTE reports are sent simultaneously to the supported unit S2, to the OMT in control of the HCT, and to the intelligence staff officer of any other tactical unit that may be affected by the information contained in the SALUTE report.

10-11. The OMT reviews the report and forwards it to the supporting HAT and supporting J/G/S2X for inclusion in the analysis picture. The supported S2 will—

- Review the information.
- Incorporate it into his unit intelligence products, as applicable.
- Forward the information to his higher echelon intelligence staff officer.
- Ensure that all affected units are notified.

10-12. Units must develop SOPs for the passing of information and intelligence to multinational units. Report writers and editors must ensure that reports that are to be shared with multinational units contain only releasable information. This will enable reports to have the widest dissemination. Arrangements are made through the C/J2X/LNO for distribution. When possible, reports to be shared with multinational units should be kept to the appropriate classification to ensure the widest dissemination of the reported information.

Basic Source Data Reports

10-13. The basic source data (BSD) reports provide the HUMINT chain with biographic and operational information related to a source. BSDs are used at all echelons to collect biographic information on all contacts. The use of BSDs and BSD formats are covered in DIAM 58-11 (S//NF).

Contact Reports

10-14. Collectors use contact reports to inform their technical chain (from OMT through J/G/S2X) of all relevant information concerning specific meetings with HUMINT sources. Information typically includes the circumstances of the contact (purpose, locations, time), the operational

matters relative to the contact (topics discussed, taskings given), reports produced as a result of the contact, and logistics expended.

Other Reports

10-15. HUMINT collectors also use a number of other reports to administer source contacts and to report information. Copies of the following reports should be maintained in the detainee's permanent file for future reference. HUMINT collectors will review these reports when planning additional collection activities; release committees or tribunals can use the reports to help evaluate if a detainee can be released or not. These reports include—

- Screening Reports. Screening reports are used to report BSDs, knowledge areas and levels, cooperation, vulnerabilities to approaches, and other relevant source information between HUMINT collectors. It is normally filled out either electronically or manually by the initial HUMINT collector to speak to a source. The screening report is normally forwarded electronically to higher echelon HUMINT collection organizations and other MI organizations that might have interest in the source. Higher echelon organizations may add information to the screening sheet extracted through subsequent screenings. Available digital screening reports contained in the HUMINT collector's mission support software (for example, BAT or CI/HUMINT Automated Management System [CHAMS]) should be used whenever possible to ensure rapid transfer of data. If screening reports have to be handwritten, the information collected should conform to theater requirements and local SOPs.
- Knowledgeability Briefs. The KB is used to inform the Intelligence Community of a source's full identity, past history, and areas of knowledge, as well as to set a suspense date for the submission of intelligence requirements. It is normally only used at the strategic and operational echelons. When completed, a KB will be classified at least Confidential in accordance with the DIA Classification Guide to protect the identity of the source. The use of KBs and the formats are covered in DIAM 58-11 (S//NF). See Figure 10-2 for an example of a short form KB that can be used for screening at all echelons, and can also be prepared and published like the full KB. This allows the entire intelligence community to see who is either in custody or to whom US intelligence has access so that SDRs can be issued to help focus the intelligence collection effort.
- Notice of Intelligence Potential (NIP). A NIP is used to inform the US Intelligence Community of the availability of a source of potential interest and to notify them of what agency has responsibility for questioning that source and where to forward questions and requests for information from that agency. The use of NIPs and the formats are covered in DIAM 58-11 (S//NF).
- Lead Development Report (LDR). The LDR is used to inform the HUMINT chain of ongoing operations directed toward a specific source. It notifies them as to what element spotted the potential source, the

current steps in assessing of the source, and the general information on the potential source.

- Interrogation Summary. An interrogation summary may be written to record relevant facts concerning the interrogation. The summary may include the attitude of the source; approach techniques that were tried and which ones were effective; incentives promised and whether or not they were delivered yet; recommended topics for further exploitation; and any other topics the HUMINT collector considers relevant. Local SOPs will dictate the use of the interrogation summary.
- Interrogation Plan. The interrogation plan is a report prepared by the HUMINT collector to organize his plan to approach and question a source. It lists collection objectives, approach techniques, preparation and liaison tasks, and interpreter usage plan. The interrogation plan also has approval blocks for interrogation supervisor approval of selected approaches and medical release for questioning. The last part of the form has termination, approach effectiveness, recommendations for further exploitation, and a summary of information obtained and reports expected to be published. Figure 10-3 is an example of an interrogation plan format.
- Termination Report. The termination report is used at all echelons to inform the technical chain of the termination of a contact relationship between a HUMINT collector and a source.
- Biographic Report. The biographic report is a formatted IIR used at all echelons to report information collected from one human source about another individual of actual or potential intelligence interest. The biographic report format is found in DIAM 58-11 (S//NF).

REPORTING ARCHITECTURE

10-16. There are three basic reporting channels (see Figure 10-1):

- The operational reporting chain consists of primarily the C2 elements for the HUMINT collection element. It includes the OMTs, unit commanders, and unit S3 and operation sections.
- The technical chain includes the OMTs, HOC, and the C/J/G/S2X, and in certain circumstances, the unit G2/S2s.
- The intelligence reporting chain includes the OMTs, HATS, C/J/G/S2Xs, and unit G2/S2s.

10-17. Many elements serve multiple and overlapping functions within the reporting architecture. Each element must be aware of its function within the architecture to ensure that information is disseminated expeditiously to the right place in the right format. This architecture should be established and published prior to implementation in order to avoid confusion.

OPERATIONAL REPORTING

10-18. Operational reporting is sent via the organic communications architecture (see Chapter 13). Operational reports are normally sent per unit SOP or based on direction from higher headquarters. HCTs normally send all

operational reports through their OMT to the command element of the unit to which they are assigned. If an HCT is attached, it will normally send its operational reports to the unit to which it is attached with courtesy copies to their assigned unit as required. If there is an administrative or logistics relationship established with the supported unit, HCTs that are in DS send the principal copy of all related administrative and logistic reports to the supported unit with a courtesy copy to their parent unit. If the HCT is operating in GS, a courtesy copy of operational reports should be forwarded to all affected unit commanders in the supported AO.

TECHNICAL REPORTING

10-19. Technical reporting includes the forwarding of source information and technical parameters of collection operations from lower to higher and the passing of tasking specifics, source information, technical control measures, and other information from higher to lower. Technical reporting is conducted through the technical chain that extends from the HCT through the OMT and Operations Section (if one exists) to the C/J/G/S2X.

INTELLIGENCE REPORTING

10-20. The key to intelligence reporting is to balance the need for accurate reporting with the need to inform affected units as quickly as possible. The J/G/S2 and MI commander are key to ensuring the right balance.

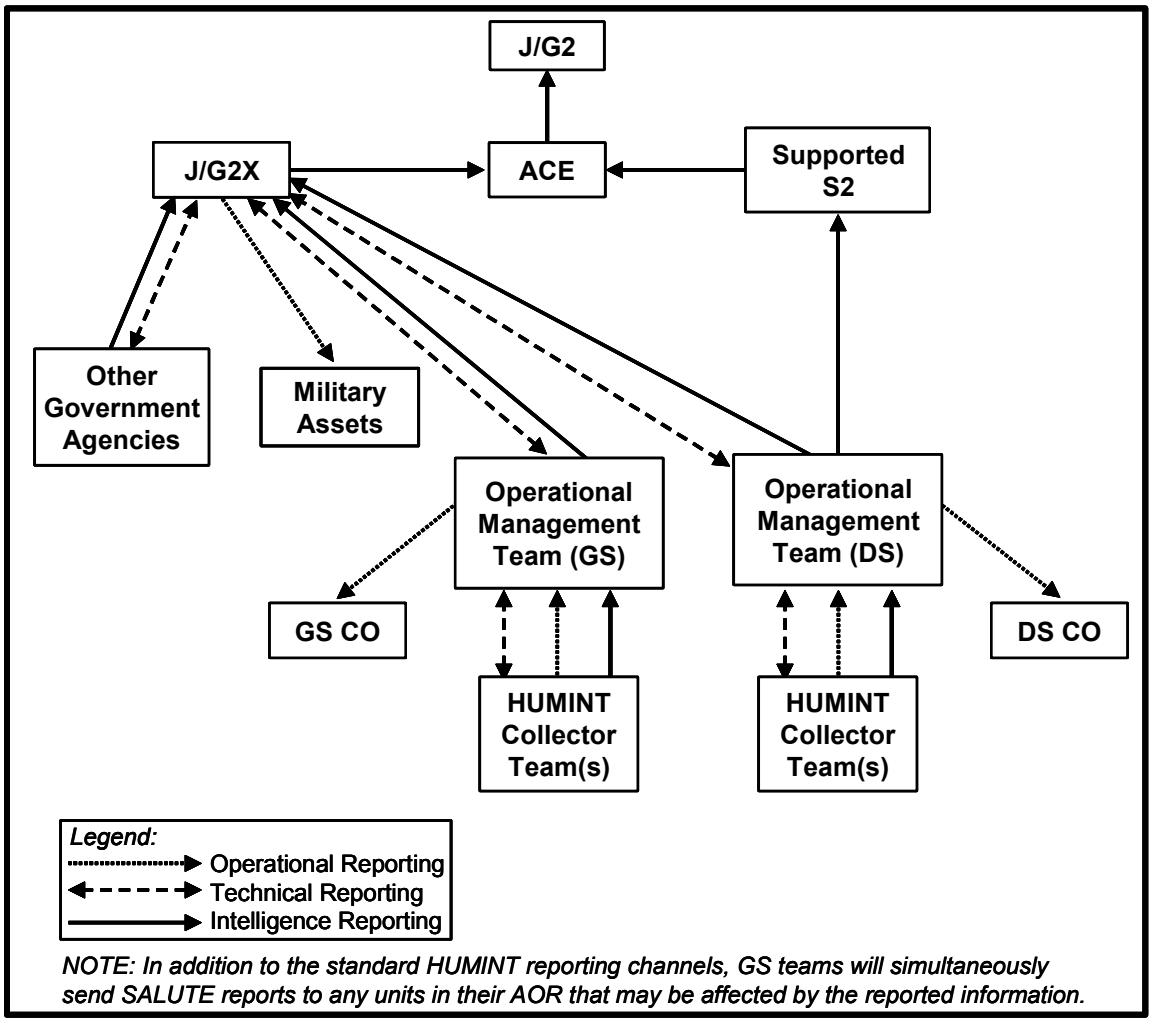


Figure 10-1. HUMINT Reporting Channels.

KB-EZ WORKSHEET

1. PERSONAL DATA:

1A. Name:

1B. Source Number (Capturing Unit):

1C. Source Number (MPs):

1D. Source Number (Other):

1E. Source Number (MI):

1F. Country of Citizenship:

1G. Birth City:

1H. Birth Country:

1I. Birth Date:

1K. Date Departed Country of Origin/Date of Capture:

1N. Last County of Residence:

1O. Language Competency:

2. Education: (Most Recent to Oldest)

2A. Military or Civilian:

2B. Dates of Attendance:

2C. Name of Institution:

2D. City Location of Institution:

2E. Country Location of Institution:

2F: Completion Status/Degree Type:

3. EMPLOYMENT: (Most Recent to Oldest)

3A. Dates of Employment:

3B. Name of Place of Employment:

3C. City Location of Place of Employment:

3D. Country of Place of Employment:

3E. Employment Duty Position:

3F. Security Clearance:

SAMPLE

Figure 10-2. KB-EZ Worksheet.

4. MILITARY SERVICE: (Most Recent to Oldest)

4A. Dates of Service:

4B. Name of Post/Base:

4C. Armed Service Component:

4D. Rank of Equivalent:

4E. Name of Unit/Group:

4F. City Location of Unit/Group:

4G. Country Location of Unit/Group:

4H. Military/Group Duty Position/Title:

4I. Security Clearance:

5. Comments: (Character, intelligence, motivation, personality, cooperativeness)

5A. CIRCUMSTANCES OF CAPTURE: Capture date, capturing unit, circumstances, documents, weapons, and equipment.

5B. ASSESSMENT: Physical condition, mental condition, intelligence, cooperation (1, 2, 3), knowledgeability (A, B, C), personality.

5C. ADDITIONAL PERSONAL INFORMATION: (Skills, experience, marital status, other).

6. NAME OF SCREENER:

SAMPLE

Theater-specific collection requirements may require modification of the KB-EZ format. Consider adding entries for:

- Race
- Ethnicity
- Tribal Affiliation
- Religion and Sect
- Language and Dialect Spoken

Entries for "Location" may need to include a village or even neighborhood.

Figure 10-2. KB-EZ Worksheet (continued).

INTERROGATION PLAN

PLANNING: **DTG:**_____

Collector Name:_____ **FRN:**_____

Detainee Name:_____

Detainee MP Number:_____ **Other Identifying Numbers (specify):** _____

Number of Times Interrogated:_____

Interrogation Objectives:_____
(Include PIR, SDR, RFI, IPSP, etc.)

Fit to undergo interrogation: YES_____ **NO** _____

Health concerns to be reported to the commander:_____

Approach Strategies (Attach separate sheet if needed for additional approaches):

Initial Approach: _____

Rationale: _____

Additional Approach: _____

Rationale: _____

Additional Approach: _____

Rationale: _____

REVIEW: Interrogation Supervisor_____ **MI Unit Commander**_____
SJA_____ **BSC (as appropriate)** _____

APPROVAL AUTHORITY:	**PRINTED NAME**	**DTG OF APPROVAL**	**SIGNATURE**
First O-6 (as required):	_____	_____	_____
Interrogation Unit OIC	_____	_____	_____
Interrogation Supervisor	_____	_____	_____

Interpreter Name and Interpretation Method: _____

Other Participants:_____

Lead Agency: _____

Recording Method:_____Monitoring Method:_____

SAMPLE

Figure 10-3. Interrogation Plan Format.

PREPARATION:

Coordinate with MP for access to the detainee.

Prepare for exploitation topics:
- Obtain appropriate map sheet(s)
- Obtain references
- Review previous reports, detainee correspondence
- Research collection topics
- Prepare questions

Prepare interrogation site (furnishings, lighting, climate, security, monitoring).

Ask Guard Questions.

Review Detainee Documentation:
- ID Card
- Capture Tag
- Documents captured with the detainee

Post-Interrogation Report

Effectiveness of Approaches:

Attitude and Behavior of Detainee:

Summary of Topics Exploited:

Expected Reports Production in Response to Requirements:

Termination:
- Reason:
- Approach Reinforced:
- Incentive Promised:
- Delivered:

Recommendation for Further Interrogation and Rationale:

- Recommended Approach(es):

- Topics for Further Exploitation (Leads):

Disposition of Source:_____

Additional Comments:_____

SAMPLE

Figure 10-3. Interrogation Plan Format (continued).

This page intentionally left blank.

Chapter 11

HUMINT Collection With An Interpreter

11-1. The use of interpreters is an integral part of the HUMINT collection effort. It is vital that the HUMINT collection skills be paired up with a qualified interpreter. Use of an interpreter is time consuming and potentially confusing. Proper use and control of an interpreter is a skill that must be learned and practiced to maximize the potential of HUMINT collection. It is also vital for the HUMINT collector to confirm that the interpreter he intends to use holds the required clearance for the level of information that will be discussed or potentially collected, and is authorized access to the detainee. This chapter deals strictly with the use of interpreters to support HUMINT collection; it is not intended to be applied to more routine uses of interpreters in support of administrative, logistical, or other operational requirements.

ADVANTAGES AND DISADVANTAGES OF INTERPRETER USE

ADVANTAGES

11-2. Interpreters are frequently a necessary aid to HUMINT collection. There are certain advantages to using an interpreter. The most obvious is that without an interpreter, a HUMINT collector without the proper language or necessary proficiency in that language is severely limited. Furthermore, if properly trained, briefed, and assessed, the interpreter can be a valuable assistant to the HUMINT collector. The interpreter—

- Probably has a greater knowledge of the local culture and language usage than could be developed by the HUMINT collector.
- Can identify language and culturally based clues that can help the HUMINT collector confirm or refute the veracity of the source's statements.
- Can interpret not only the literal meaning of a statement but also the intent and emotion of a sentence.

DISADVANTAGES

11-3. There are, however, several significant disadvantages to using interpreters. Disadvantages may include—

- A significant increase in time to conduct the collection. Since the interpreter must repeat each phrase, the time for a given questioning session or meeting is normally at least doubled.
- Since there is now a third person in the communications loop, the potential for confusion or misunderstanding increases significantly. This is especially true when the interpreter is deficient in his command of either language.

- The establishment of rapport and the use of some approach techniques (see Chapter 8) are made difficult or even impossible when working through an interpreter.
- The ability of the HUMINT collector to interpret the source's veracity through the analysis of word usage, nuances of speech, and body language is curtailed.
- The interpreter will have his own set of biases that could influence the manner in which the dialogue is interpreted.
- The source may be culturally biased against the interpreter. This is especially possible if the interpreter was locally hired and is of a different ethnic, social, or religious group than the source.
- The interpreter may be culturally biased against the source and intentionally misinterpret the meaning to obtain a desired effect.
- There may be mission or subject matter classification problems involved.

CAUTIONS

11-4. Be careful of comments made in the presence of your interpreter. Although you plan comprehensively with your interpreter, you should only share information with your interpreter on a need-to-know basis. Obviously the exchange of information concerning the "what, where, when, with whom, and how" of each meeting must be discussed with your interpreter, but sometimes the "real why" is none of his business! You may be meeting with a source or contact because the commander believes this individual has lied. The real purpose (the why) of the meeting is to pose control questions and to determine whether the source or contact lied in the past or whether there was simply a miscommunication.

11-5. Be careful of sensitive or personal conversations when the interpreter is present. This applies to conversations en route to or from meetings, conversations over lunch or dinner in the operational area, and conversations in the team area. It is easy to get used to the presence of the interpreter and to overlook his presence. An interpreter is a necessary tool but we must remember that most are only very lightly screened for the sensitive access they have. If your interpreter turned out to be working for the other side, what information beyond "the necessary" could he provide?

METHODS OF INTERPRETER USE

11-6. There is a basic method and advanced method of interaction between the HUMINT collector and the interpreter. As the collector and the interpreter become experienced at working together and gain confidence in each other's abilities, they may use more advanced interactive techniques. It is the HUMINT collector's decision whether or not to use more advanced techniques.

BASIC METHOD

11-7. The basic method of interaction is used when—

- The interpreter and HUMINT collectors have not worked together extensively.
- The interpreter has language skills but no interpreter training or experience.
- The interpreter's skill in English or the target language is suspect.
- The HUMINT collector has limited experience using an interpreter.
- The interpreter's capabilities, loyalty, or cultural knowledge are not known or suspect.

11-8. Using the basic method, the interpreter is used solely as an interpretation device. When initial contact is made, the interpreter instructs the source to maintain eye contact with the HUMINT collector. The interpreter is briefed on the general course of the collection but usually is not advised of the specific purpose or collection goals. While the interpreter will be instructed to reflect the attitude, behavior, and tone of voice of both the collector and the source, he is told to *not* interpose comments or personal opinions at all in the conversation.

11-9. The questioning phase is conducted in the same way it would be if no interpreter were used with the obvious increase in time due to the interpretation. The interpreter uses the same person and tense as the HUMINT collector or source and neither adds nor subtracts anything from the dialogue. He does his best to fade into the background. When reports are written, the interpreter will only be asked questions based on the actual translation of the dialogue.

ADVANCED METHOD

11-10. The advanced method of interaction requires additional training on the part of the HUMINT collector and the interpreter, extensive experience working together, and a rapport between the HUMINT collector and the interpreter. The HUMINT collector must trust both the capabilities and the judgment of the interpreter. At this level of interaction, the interpreter becomes a more active participant in the HUMINT activities. The HUMINT collector remains in charge and makes it clear to the interpreter that he (the HUMINT collector) is responsible for the substance and direction of the questioning. The interpreter is normally briefed as to the specific goals of the collection.

11-11. The interpreter becomes a more active participant in the approach and termination phases to the point of even making planned comments to the source supportive of the HUMINT collector's approach. For example, if the HUMINT collector is using an incentive approach, the interpreter in an aside to the source can tell him that the HUMINT collector always keeps his promises. This type of technique should only be used if both planned and rehearsed.

11-12. During the questioning phase, the interpreter supports the collector by not only translating the word of the source but also cueing the collector when there are language or culturally based nuances to what the source is

saying that might add credence or doubt as to the veracity of the statements. For example, the interpreter could point out that although the source claims to be a factory worker, his language use indicates that the source has a university education. In another example, the interpreter could indicate that the dialect or pronunciation that the source is using does not match the area that he claims to be from. During report writing, the interpreter supports the HUMINT collector by not only answering questions on the literal interpretation but also adds, when appropriate, comments on the significance of both what was said and how it was said.

SOURCES OF INTERPRETERS

11-13. There are almost never sufficient interpreters to meet all unit mission requirements. Interpreters in support of HUMINT collection require a security clearance and knowledge of the operational situation. While any qualified interpreter can be used to support HUMINT collection, the HUMINT collectors maximize the collection potential if the interpreter has received specific training. The number of interpreters needed to support a HUMINT collection mission is METT-TC driven based primarily on the number of HUMINT collectors, the dispersion of the HUMINT collectors in the AO, and the number of sources. Normally one interpreter for every two non-language qualified HUMINT collectors is sufficient; however, in situations where a large number of high-value sources must be questioned in a limited time, a ratio of 1 to 1 may be required. Interpreters are obtained from within the military and from the US and local civilian populations or other English-speaking countries.

MILITARY

11-14. There are many soldiers, including non-US citizens, who have native language abilities due to their upbringing. Their parent unit may identify these language abilities, or these soldiers may volunteer their abilities when a contingency arises. The ARNG, USAR, other US military services, and even coalition militaries, have language-trained and certified personnel in Military Intelligence MOSs, such as 98G or 09L, who may be called upon to serve as interpreters for the HUMINT collection effort.

CIVILIAN

11-15. Civilian corporations may be contracted by the military to provide interpreters for an operation. These interpreters are divided into three categories:

- CAT I Linguists - Locally hired personnel with an understanding of the English language. These personnel undergo a limited screening and are hired in-theater. They do not possess a security clearance and are used for unclassified work. During most operations, CAT I linguists are required to be re-screened on a scheduled basis. CAT I linguists should not be used for HUMINT collection operations.
- CAT II Linguists - US citizens who have native command of the target language and near-native command of the English language. These personnel undergo a screening process, which includes a national

agency check (NAC). Upon favorable findings, these personnel are granted an equivalent of a Secret collateral clearance. This is the category of linguist most used by HUMINT collectors.

- CAT III Linguists - US citizens who have native command of the target language and native command of the English language. These personnel undergo a screening process, which includes a special background investigation (SBI). Upon favorable findings, these personnel are granted an equivalent of a Top Secret (TS) clearance. CAT III linguists are used mostly for high-ranking official meetings and by strategic collectors.

INTERPRETATION TECHNIQUES

11-16. During the planning and preparation phase, the HUMINT collector, in collaboration with the interpreter, selects a method of interpretation. There are two methods:

- Alternate Interpretation. The interpreter listens to the entire phrase, sentence, or paragraph. The interpreter then translates it during natural pauses in speech.
- Simultaneous Interpretation. The interpreter listens to the source and translates what he says, just a phrase or a few words behind. The HUMINT collector should select the simultaneous method only if all the following criteria are met:
 - The sentence structure of the target language is parallel to English.
 - The interpreter can understand and speak English as well as the target language with ease.
 - The interpreter has special vocabulary skills for the topics to be covered.
 - The interpreter can easily imitate the HUMINT collector's tone of voice and attitude for the approaches and questioning technique selected.
 - Neither the collector nor the interpreter tends to get confused when using the simultaneous method of interpretation.

11-17. If any of the above-mentioned criteria in the simultaneous method cannot be met, the HUMINT collector should use the alternate method. The alternate method should also be used when a high degree of precision is required.

TRAINING AND BRIEFING THE INTERPRETER

11-18. The HUMINT collector will need to train an individual who has no interpreter experience as well as remind a trained and certified interpreter of the basic interpreter requirements. The requirements include—

- Statements made by the interpreter and the source should be interpreted in the first person, using the same content, tone of voice, inflection, and intent. The interpreter must not interject his or her own personality, ideas, or questions into the interview.

- The interpreter should inform the HUMINT collector if there are any inconsistencies in the language used by the source. The HUMINT collector will use this information in his assessment of the source.
- The interpreter needs to assist with the preparation of reports and administrative documents relevant to the source and meeting.

11-19. Once the HUMINT collector has chosen a method of interpretation, he must brief the interpreter. This briefing must cover—

- The current situation.
- Background information on the source (if available).
- The administrative particulars of the meeting such as where it will be held, the room setup, how long it will last.
- The specific positioning of the interpreter, collector, and source.
- The general or (if advanced method of interaction is being used) the specific collection objectives.
- The selected approach and possible alternate approaches that the HUMINT collector plans on using. If time allows, the collector and interpreter should rehearse the approaches.
- Any special topic or technical language that is anticipated. If time allows, the interpreter should research any anticipated technical vocabulary with which he is unfamiliar.

11-20. Throughout the briefing, the HUMINT collector fully and clearly answers questions the interpreter may have. This helps ensure the interpreter completely understands his role in the HUMINT collection process. With a more advanced interaction plan, the HUMINT collector and the interpreter should "wargame" their plan and rehearse their actions as necessary.

PLACEMENT OF THE INTERPRETER

11-21. The interpreter should be placed in a position that enhances the mood or general impression that the HUMINT collector wants to establish. When dealing with detainees or EPWs, the HUMINT collector generally wants to establish a dominant position, maintain a direct relationship with the source, and increase or at least maintain the anxiety level of the source. Having the HUMINT collector and the source facing each other with the interpreter located behind the source normally facilitates this. It allows the HUMINT collector to maximize control of both the source and interpreter. If desired, having the interpreter enter the room after the source, so the source never sees the interpreter, can further heighten the anxiety of the source.

11-22. Having the interpreter sit to the side of the HUMINT collector creates a more relaxed atmosphere. This is the norm for debriefings and official meetings. Having the interpreter at his side also facilities "off line" exchanges between the HUMINT collector and the interpreter. The collector should avoid having the interpreter sit beside the source since this has a tendency of establishing a stronger bond between the source and the interpreter and makes "off line" comments between the collector and the interpreter more difficult.

11-23. When conducting source meetings in a public setting, a more natural appearance is desirable. The seating needs to conform to the norm at the location where the meeting is taking place. For example, if meeting at a restaurant, the HUMINT collector, interpreter, and source will sit naturally around the table.

INTERACTIONS WITH AND CORRECTION OF THE INTERPRETER

11-24. The HUMINT collector must control the interpreter. He must be professional but firm and establish that he is in charge. During a questioning session, the HUMINT collector corrects the interpreter if he violates any standards that the pre-mission briefing covered. For example, if the interpreter interjects his own ideas into the meeting, he must be corrected. Corrections should be made in a low-key manner as to not alienate the interpreter, interrupt the flow of the questioning, or give the source the impression that there is an exploitable difference of opinion between the HUMINT collector and the interpreter. At no time should the HUMINT collector rebuke the interpreter sternly or loudly while they are with the source. The HUMINT collector should never argue with the interpreter in the presence of the source. If a major correction must be made, the HUMINT collector should temporarily terminate the meeting and leave the site temporarily to make the correction. The HUMINT collector needs to document any difficulties as part of his interpreter evaluation. The HUMINT collector must always ensure that the conduct and actions of the interpreter are within the bounds of applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs.

11-25. The HUMINT collector must be alert for any signs that the interpreter is not performing as required. The following are some indicators of possible problems.

- Long-to-short. If you take 20 seconds to express yourself and the interpreter reduces it to a 3-second translation, it may indicate that something has been omitted, and you should not proceed until you have resolved the issue. There is nothing wrong with stating that you would "prefer" the interpreter translate everything that was just said. If you have trained your interpreter properly, this should not be an issue. If it arises even with the training you have given the interpreter, then it has significance and you must not let it pass.
- Short-to-long. If you take 5 seconds to express yourself and the interpreter expands it to a 30-second translation, it may indicate that something has been added, and you should not proceed until you have resolved the issue.
- Body-language shift. If the interpreter's body language suddenly has a significant shift from his normal behavior, you should look for the reason. (It is advisable for you to determine a base line of behavior for your interpreter to facilitate recognition of the changes.) Perhaps he is reluctant to translate what you just said. Be aware that the body shift

means that something is happening—your task is to find out what it means.

- Unusual pauses. Look for a longer delay than usual before the translation begins. Unless it is a vocabulary or concept issue, the long delay means that the interpreter is "thinking" before he translates. Any thinking beyond what is needed to translate, as closely as possible, what was just said represents a potential problem. Again, you should establish a base line of behavior for your interpreter so you can recognize these unusual pauses.
- "Wrong" reactions. If you say something humorous that should provoke a positive response from the source, and you do not get that response, then you should wonder if the message got through. If the source becomes upset in response to something (positive) you said, then you should begin to wonder what message was passed by the interpreter. Did you fail to express yourself clearly, or was it an accidental or deliberate mistranslation?

11-26. A trusted linguist should periodically review the accuracy of the interpreter's translations by monitoring an interrogation or debriefing and critiquing the monitored interpreter's performance.

INTERPRETER SUPPORT IN REPORT WRITING

11-27. The interpreter assists the HUMINT collector in preparing all required reports. He may be able to fill gaps and unclear details in the HUMINT collector's notes. He may also assist in transliterating, translating, and explaining foreign terms.

EVALUATING THE INTERPRETER

11-28. After submitting all reports, the HUMINT collector evaluates the performance of his interpreter. This should be done in writing, and copies should be given to the interpreter and placed on file with the individual managing the HUMINT collection portion of the interpreter program. The interpreter program manager needs to develop a standard evaluation format for inclusion in the unit SOP. The evaluation forms should note at a minimum:

- Administrative data (for example, date, time, interpreter's name).
- Strengths and weaknesses of the interpreter with any problems and corrective actions taken.
- Type of interpretation used (simultaneous or alternate).
- Type of HUMINT operation the interpretation was supporting (that is, an interrogation, a debriefing, a liaison meeting).
- Ability or lack of ability of the interpreter to use specific technical language that may have been required.
- Name or collector number of the HUMINT collector.

11-29. The interpreter program manager uses these forms to decide on future use of the interpreters, to develop training programs for the interpreters, and to assign interpreters to make maximum use of their specific capabilities.

The HUMINT collector should also review these files before using an unfamiliar interpreter.

MANAGING AN INTERPRETER PROGRAM

11-30. Units requiring interpretation support need to identify an individual or individuals to manage the interpreter program. In most units, this will be someone in the G3/S3 section. Division and Corps-level units will have a language manager. In MI units whose specific function is HUMINT collection, it will normally be a senior Warrant Officer within that unit. The functions of the interpreter program manager include but are not limited to—

- Consolidating and prioritizing interpreter requirements.
- Coordinating with G2 or INSCOM to contract for qualified interpreters.
- Coordinating with the G1/S1 to identify personnel in the unit with language skills who can be used as interpreters.
- Coordinating with the G1/S1 and G5 to obtain qualified local-hire interpreters.
- Coordinating with G2/S2 for clearances.
- Coordinating with the G3/S3 to establish training for both the interpreters and those that will be using interpreters.
- Coordinating with the G3/S3 for language testing of the interpreters in both English and the target language as required.
- Coordinating with the G1/S1 and G4/S4 to ensure that all administrative and logistical requirements for the interpreters are met.
- Establishing and maintaining the administrative, operational, and evaluation files on the interpreters.
- Assigning or recommending the assignment of interpreters to operational missions based on their specific capabilities.

This page intentionally left blank.

PART FOUR

Analysis and Tools

Part Four discusses HUMINT analysis and the automation and communication tools needed to support the HUMINT collection effort.

HUMINT analysis supports operational planning and provides direction to HUMINT collection operations. Analysts determine if information from a single human source is internally consistent based on factors such as placement and access of source, prior information from the source, and existing holdings. Source analysis is used to determine if the information from a source is complete, truthful, and responsive to collection requirements. Operational analysis consists of those actions taken to determine how to best meet requirements.

Modern automation and communications systems are vital to HUMINT collection. Real-time collaboration, detailed operational planning and ISR integration, as well as enhanced collection and source exploitation tools, must support team efforts. Emerging technology continues to allow the entire HUMINT collection system to operate more effectively. Commanders must be prepared to supply their HUMINT collection assets with the best possible technology.

Chapter 12

HUMINT Analysis and Production

12-1. Analytical processes provide information to support the commander, his staff, and his unit. Analysis is an integral part of HUMINT collection. Analysis occurs throughout the HUMINT collection process but can be divided into four primary categories: analytical support to operational planning and targeting, operational analysis and assessment, source analysis, and single-discipline HUMINT analysis and production.

ANALYTICAL SUPPORT TO OPERATIONAL PLANNING

12-2. Several elements provide analytical support at various echelons, including the following:

- The HAT is subordinate to the G2 ACE. The HAT supports the G2 in developing IPB products and in developing and tailoring SIRs to match HUMINT collection capabilities.

- The HAC is subordinate to the C/J/G/S2X and functions in the same capacity for the C/J/G/S2X as the HAT does for the ACE.
- The HOC of the C/J/G/S2X supports the C/J/G/S2 and C/J/G/S2X in the identification of HUMINT collection opportunities, the development of taskings and RFIs for HUMINT collection assets, as well as the development of a HUMINT database.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

12-3. The HAT assists the G2 in the identification and characterization of the human component of operations and its effects on friendly and enemy operations. As part of its assistance to the G2, the HAT compiles and analyzes data about the local civilian population including its political, ethnic, religious, cultural, tribal, economic, and other social components. It carefully examines the various component groups and their predicted reaction to friendly force operations.

12-4. The HAT also provides input to all-source analysis by identifying specific actions and motivational factors that should strengthen the local population's support of the US or at least weaken its support of the enemy and by providing information on transient (refugees, DPs, third-country nationals) population and its effects on friendly and enemy operations. In addition to the above, the HAT—

- Closely examines the current and potential threat to identify all factors, such as morale, motivation, training, and beliefs that would affect both positively and negatively on enemy and opposing force capabilities.
- Identifies formal and informal leaders of hostile, neutral, and friendly groups and how their influence is likely to affect operations.
- Develops overlays, databases, and matrices, as required, to support IPB. These overlays may represent a wide variety of intelligence issues, including battlefield infrastructure (for example, electrical power grid), population density, ethnic, religious, or tribal affiliation, and no-strike or collateral damage.
- Provides its products to the C/J/G/S2, the all-source analysts and CI analysts of the ACE, the HOC, the C/J/G/S2X, and HUMINT collection units as required.

ISR TASK DEVELOPMENT

12-5. The HAT and the C/J/G/S2X support the C/J/G/S2 by expanding the PIRs that can be answered through HUMINT collection into ISR tasks that can be answered by a human source and that can be tasked to a specific collection entity. The HAT and the C/J/G/S2X provide this information to support the development of the HUMINT collection plan and its integration into the overarching ISR plan. The HAT normally establishes a list of prioritized standing indicators, and supplements this with ISR tasks developed to answer specific PIRs. The standing indicators are incorporated into the ACE's all-source analysis team's list of indicators that point to a pattern or COA. Each standing indicator is integrated with other indicators

and factors so that analysts can detect patterns and establish threat intentions.

SUPPORT TO HUMINT TASKING

12-6. The C/J/G/S2X supports the C/J/G/S2 and the C/J/G/S2 requirements manager by developing tasking for specific organic or attached HUMINT collection assets and by developing requests and coordinating for support from higher and lateral echelon HUMINT collection elements. The C/J/G/S2X matches specific collection requirements to collection units and sources. If current sources cannot answer the requirement, he develops profiles for new sources that guide the collection teams in the development of new sources. The C/J/G/S2X also determines the best method to achieve collection requirements. The C/J/G/S2X supplies any required technical support to the HUMINT operations section, OMTs, and HCTs.

HUMINT DATABASE DEVELOPMENT

12-7. The C/J/G/S2X maintains the source database, which receives input from HUMINT collection and CI operations. The C/J/G2X is responsible for maintaining the source database.

OPERATIONAL ANALYSIS AND ASSESSMENT

12-8. Operational analysis consists of those actions taken to determine how to best meet requirements. Assessment evaluates the effectiveness of the requirement effort. Operational analysis begins with the C/J/G/S2X when he determines the best collection assets and sources needed to answer collection requirements. For **analysis**, the C/J/G/S2X section and specifically the HOC—

- Provides higher echelon coordination and deconfliction for collection operations.
- Provides required technical support to the HUMINT operations sections, OMTs, and HCTs.
- Facilitates feedback and evaluations.

12-9. For **assessment**, the C/J/G/S2X section and specifically the HOC—

- Monitors all HUMINT reporting to ensure that requirements are being met.
- Refocuses efforts of assigned assets as needed.

12-10. The HUMINT operations section (if one exists) and the OMTs of tasked collection units determine which HCTs are best suited to meet specific collection requirements. They also conduct operational coordination for the HCT, provide technical support, and monitor all reporting to ensure that reports are properly formatted and support collection requirements. The team leader of the tasked HCT selects the specific collectors and sources to meet collection requirements, reviews the collection plan, provides technical support to the collectors, coordinates with the supported unit, and monitors all team reporting for format and content. He identifies additional lines of questioning and approaches required to fulfill collection requirements.

SOURCE ANALYSIS

12-11. Source analysis involves the actions taken to determine if information from a single human source is internally consistent based on factors such as placement and access of source, prior information from the source, and existing holdings. Source analysis is used to determine if the information from a source is complete, truthful, and responsive to collection requirements. Preliminarily source analysis is the responsibility of the individual HUMINT collector.

12-12. The HUMINT collector evaluates all source statements within the context of the information known about the source and the current situation to determine both the veracity and the validity of source statements. That is not to say that the HUMINT collector ignores any information that does not fit into expected pattern; rather that he treats that information with skepticism and uses appropriate questioning methodology to validate the statements (see Chapter 9). Source analysis is supported by the HCT leader, the OMTs, and the HOC. Each echelon reviews the intelligence and operational reports, identifies inconsistencies, evaluates veracity, and recommends additional lines of questioning as appropriate.

12-13. Analysts can assign an alphanumeric designator to collected information based on an analyst's determination of the reliability of the source and the probable accuracy of the information reported. A letter from A to F is assigned reflecting the level of reliability, with A representing the highest degree of reliability. The letter designation is then coupled with a number from 1 to 6. The number 1 represents confirmed intelligence and the numbers 2 through 6 represent increasing degrees of uncertainty as to the veracity of the information. A complete explanation if this rating system is contained in Appendix B. [NOTE: This system of labeling the reliability of sources and their reported information should not be confused with the alphanumeric rating scheme for source-screening operations as described in Chapter 6.]

SINGLE-DISCIPLINE HUMINT ANALYSIS AND PRODUCTION

12-14. Single-discipline HUMINT analysis involves the actions taken to evaluate the information provided by all HUMINT sources at a given echelon to determine interrelationships, trends, and contextual meaning. While called "single discipline," the analyst reviews and incorporates, as necessary, information from other disciplines and all-source analysis to provide a contextual basis for the HUMINT analysis. Single-discipline HUMINT analysis is conducted primarily by the HAT of the ACE. HUMINT operations sections and OMTs also conduct analysis to a lesser degree, based on the information from HUMINT sources at their echelon.

12-15. Analysis does more than simply restate facts. The analyst formulates a hypothesis based on available data, assesses the situation, and explains what the data means in logical terms that the user can understand. There are two basic thought processes used by analysts to study problems and reach conclusions: induction and deduction.

- Induction is the process of formulating hypotheses on the basis of observation or other evidence. It can best be characterized as a process of discovery when the analyst is able to establish a relationship between events under observation or study. Induction, or plausible reasoning, normally precedes deduction and is the type of reasoning analysts are required to perform most frequently.
- Deduction is the process of reasoning from general rules to particular cases. The analyst must draw out, or analyze, the premises to form a conclusion. Deductive reasoning is sometimes referred to as demonstrative reasoning because it is used to demonstrate the truth or validity of a conclusion based on certain premises.

ANALYTICAL TECHNIQUES AND TOOLS

12-16. There are three basic analytical techniques and automated tools that are particularly useful to single-discipline HUMINT analysis. Each of these tools takes fragmented bits of information and organizes them to create a chart or graph that can easily be read. They are the time event chart, matrices, and the link analysis diagram. HUMINT collectors and analysts can use automated computer programs such as Analyst Notebook or Crime Link to produce these tools or they can create them on paper. Computer programs are faster to use than previous methods and have the added advantage of producing a product that can be shared easily and rapidly over networks and portals. The diagrams in this chapter represent the tools that can be produced using automated programs.

Time Event Chart

12-17. A time event chart is a method for placing and representing individual or group actions in chronological form. It uses symbols to represent events, dates, and the flow of time. Normally, triangles are used to depict the beginning and end of the chart and may be used within the chart to indicate particularly critical events such as an ideological shift or change. Rectangles, used as event nodes, store administrative data and indicate significant events or activities. Drawing an "X" through the event node may highlight noteworthy or important events. Each of these symbols contains a sequence number, date (day, month, and year of the event), and may, if desired, contain a file reference number. The incident description written below the event node is a brief explanation of the incident and may include team size and type of incident. Arrows indicate time flow. By using these symbols and brief descriptions, it is possible to analyze the group's activities, transitions, trends, and particularly operational patterns in both time and activity. If desired, the event nodes may be color coded to indicate a particular event or type of event to aid in pattern recognition. The time event chart is the best analytical tool for pattern analysis. The example at Figure 12-1 depicts the history of the group, including most major players, which carried out the World Trade Center bombing in February 1993.

Matrices

12-18. Construction of a matrix is the easiest and simplest way to show the relationships between a number of similar or dissimilar associated items. The items can be anything that is important to a collection effort such as people, places, organizations, automobile license plates, weapons, telephone numbers, or locations. In analysis, matrices are often used to identify "who knows whom," or "who has been where or done what" in a clear concise manner. There are two types of matrices used in human analysis: the association matrix, used to determine existence of relationships between individual human beings, and the activities matrix, used to determine connectivity between individuals and any organization, event, address, activity, or any other non-personal entity. The graphics involved in constructing the two types of matrices differ slightly, but the principles are identical.

12-19. The association matrix (Figure 12-2) shows connections between key individuals involved in any event or activity. It shows associations within a group or associated activity. Normally, this type of matrix is constructed in the form of an equilateral triangle having the same number of rows and columns. Personalities must be listed in exactly the same order along both the rows and columns to ensure that all possible associations are correctly depicted. An alternate method is to list the names along the diagonal side of the matrix. This type of matrix does not show the nature, degree, or duration of a relationship, only that a relationship exists. The purpose of the matrix is to show the analyst who knows whom and who are suspected to know whom. In the event that a person of interest dies, a diamond is drawn next to his or her name on the matrix.

12-20. The analyst uses a dot or closed (filled-in) circle to depict a strong or known association. A known association is determined by direct contact between one or more persons. Direct contact is determined by several factors. *Direct associations* include—

- Face-to-face meetings.
- Telephonic conversations in which the analyst is sure who was conversing with whom.
- Members of a cell or other group who are involved in the same operations.

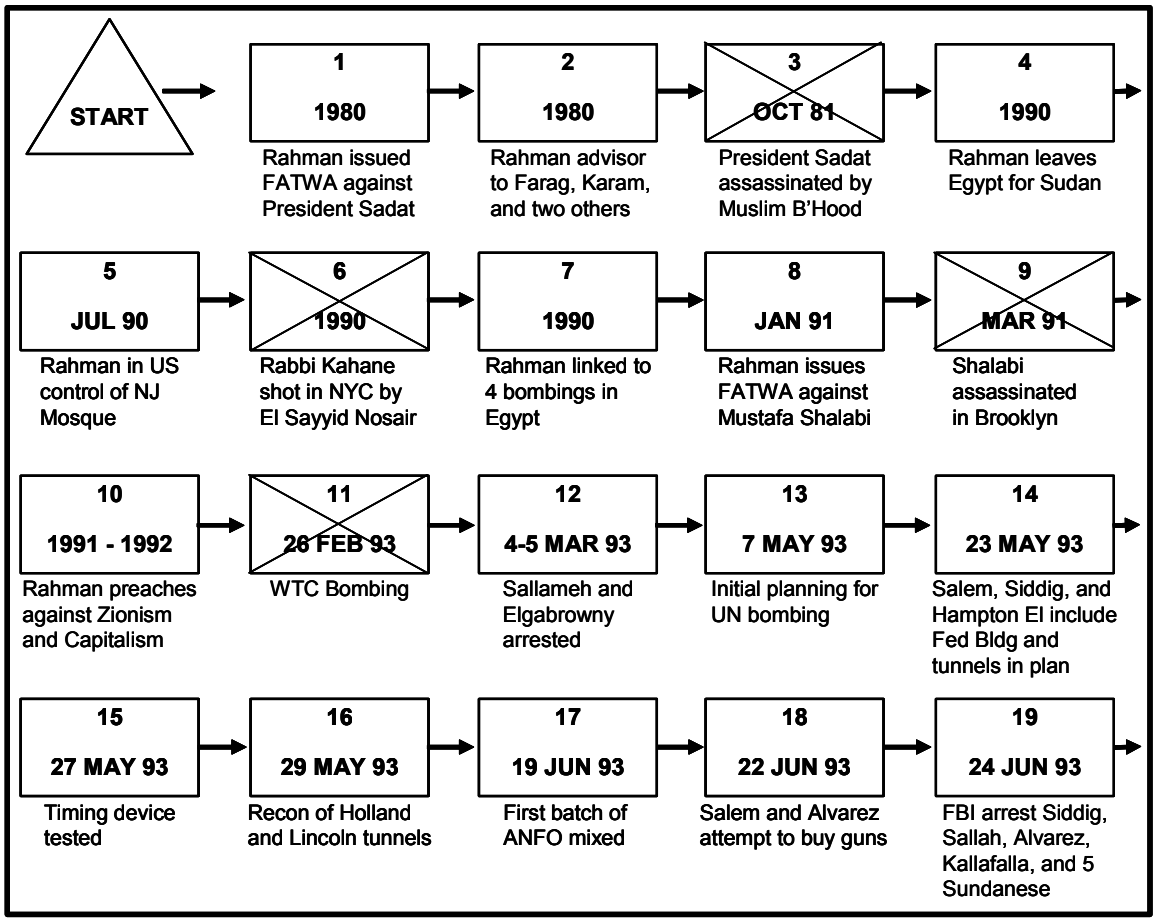


Figure 12-1. Example of a Time Event Chart.

12-21. Suspected or weak associations are those associations in which there are indicators that individuals may have had associations but there is no way to confirm that association; this is depicted with an open circle. Examples of *suspected associations* are—

- A known party calling a known telephone number (the analyst knows to whom the telephone number is listed) but it cannot be determined with certainty who answered the call.
- A face-to-face meeting where one party can be identified, but the other party can only be tentatively identified.

12-22. The rationale for depicting suspected associations is to get as close as possible to an objective analytic solution while staying as close as possible to known or confirmed facts. If a suspected association is later confirmed, the appropriate adjustment may be made on the association matrix. A secondary reason for depicting suspected associations is that it may give the analyst a focus for tasking limited intelligence collections assets in order to confirm the suspected association. An important point to remember about using the association matrix is that it will, without modification, show only the

existence of relationships; not the nature, degree, or duration of those relationships.

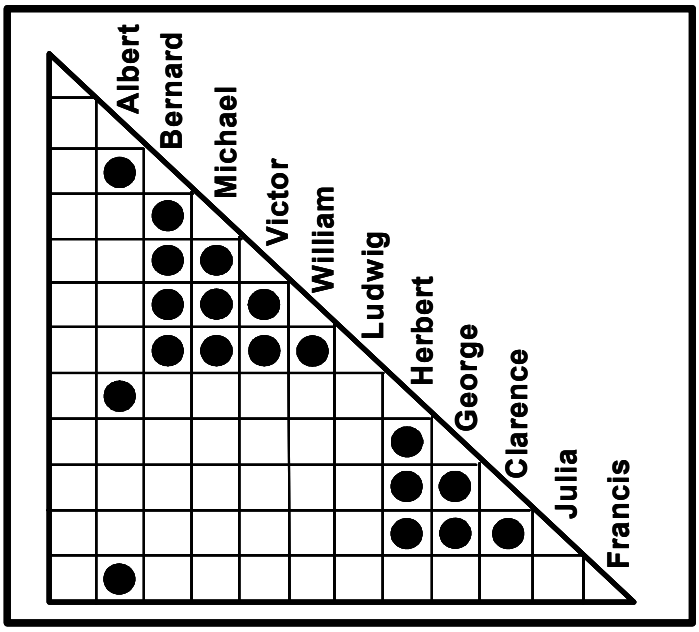


Figure 12-2. Example of an Association Matrix.

12-23. The activities matrix (Figure 12-3) is a rectangular array of personalities compared against activities, locations, events, or other appropriate information. The kind and quality of data that is available to the collector determines the number of rows and columns and their content. The analyst may tailor the matrix to fit the needs of the problem at hand or he may add to it as the problem expands in scope. This matrix normally is constructed with personalities arranged in a vertical listing on the left side of the matrix, and events, activities, organizations, addresses, or any other common denominator arranged along the bottom of the matrix. This matrix is critical for the study of a group's internal and external activities, external ties and linkages, and even modus operandi. As with the association matrix, confirmed or "strong" associations between individuals and non-personal entities are shown with a solid circle or dot, while suspected or "weak" associations are illustrated by an open circle.

12-24. Using matrices, the analyst can pinpoint the optimal targets for further intelligence collection, identify key personalities within an organization, and considerably increase the analyst's understanding of an organization and its structure. Matrices can be used to present briefings or to store information in a concise and understandable manner within a database. Matrices augment but cannot replace SOPs or standard database files. It is possible, and sometimes productive, to use one matrix for all associations. This is done routinely using the automated systems mentioned in paragraph 13-6.

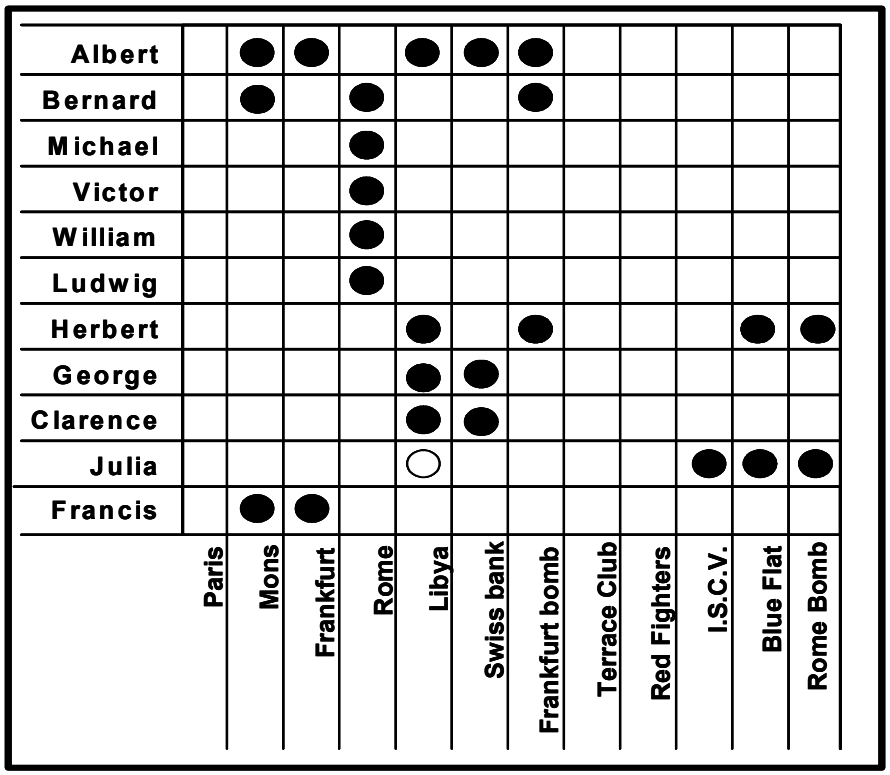


Figure 12-3. Example of an Activities Matrix.

12-25. The link analysis diagram (Figure 12-4) shows the connections between people, groups, or activities. The difference between matrices and link analysis is roughly the same as the difference between a mileage chart and a road map. The mileage chart (matrix) shows the connections between cities using numbers to represent travel distances. The map (link analysis diagram) uses symbols that represent cities, locations, and roads to show how two or more locations are linked to each other.

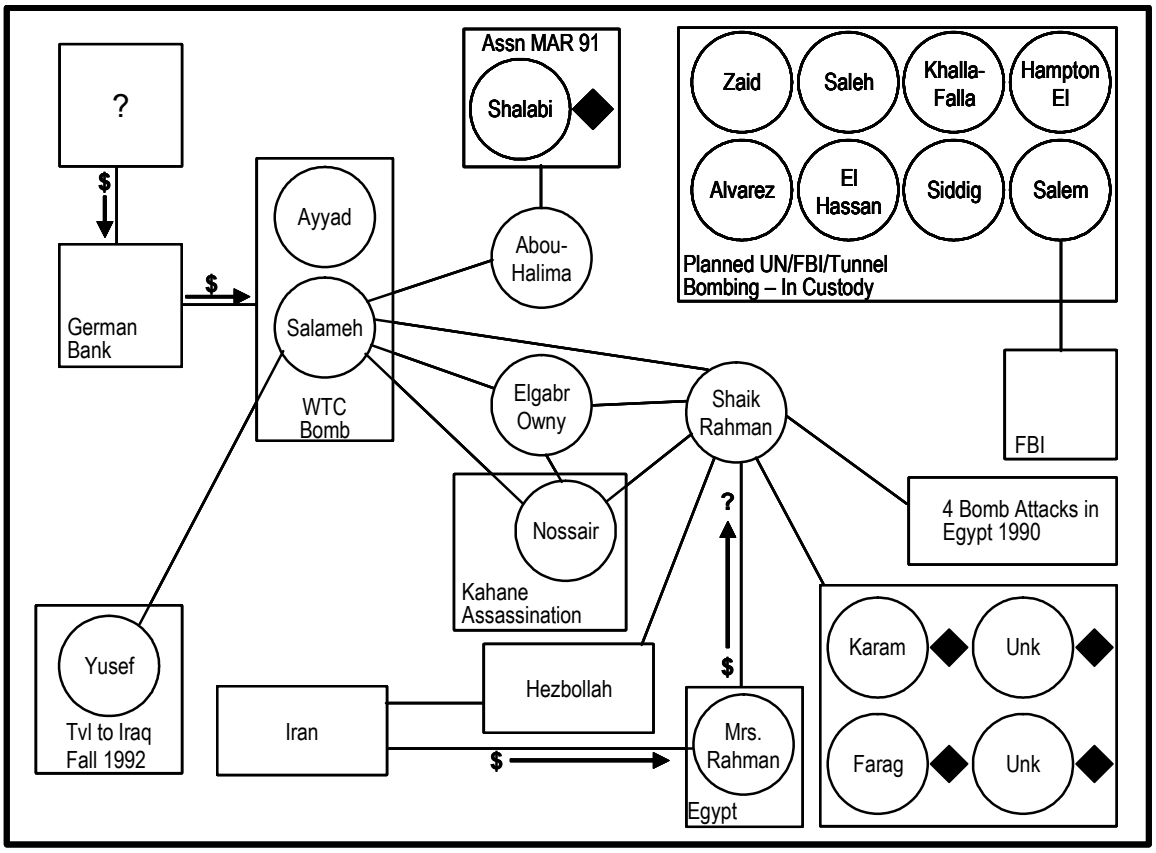
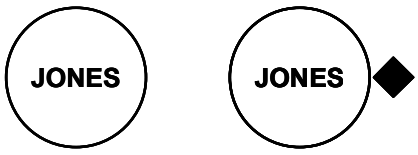


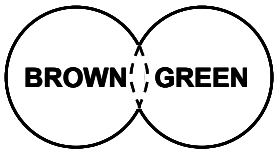
Figure 12-4. Example of a Link Analysis Diagram.

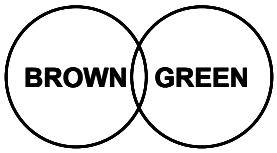
12-26. As with construction of association matrices, there are certain rules of graphics, symbology, and construction that must be followed. Standardization is critical to ensuring that everyone constructing, using, or reading a link analysis diagram understands exactly what the diagram depicts. Circles and lines are arranged so that no lines cross whenever possible. Often, especially when dealing with large groups, it is very difficult to construct a line diagram in which no lines cross. In these cases, every effort should be made to keep the number of crossings at an absolute minimum. The standard rules are as follows:

- Persons are shown as open circles with the name written inside the circle. Deceased persons are depicted in either open circles, with a diamond next to the circle representing that person (as in Figure 12-4) or as open diamonds with the name written inside the diamond.



- Persons known by more than one name (alias or AKA) are shown as overlapping circles with names in each circle (as shown below) or both names are simply listed in the same circle. If the alias is suspected, a dotted line is used to depict the intersection. If the alias is confirmed, the intersection is shown with a solid line.

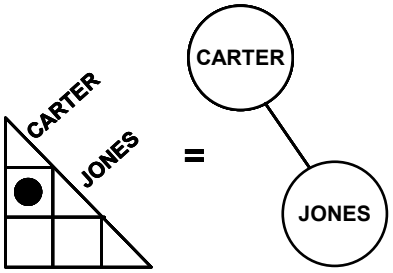


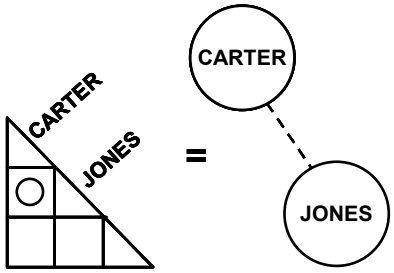


- Non-personal entities (organizations, governments, events, locations) are shown as appropriately labeled rectangles.

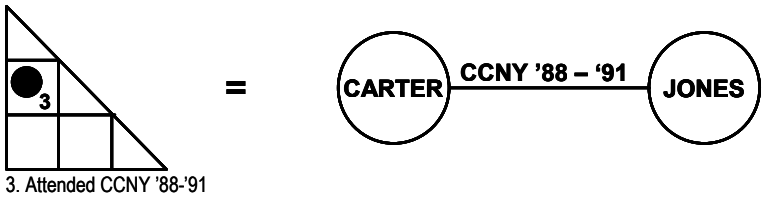


- Solid lines denote confirmed linkages or associations and dotted lines show suspected linkages and associations.



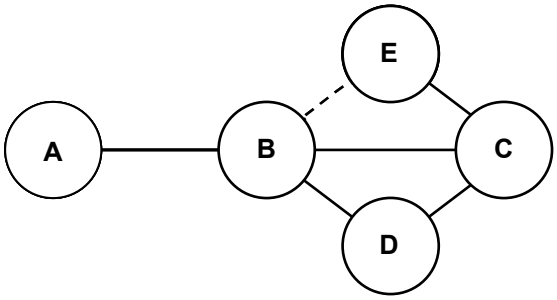


- Footnotes on the matrices can be shown as a brief legend on the connectivity line.



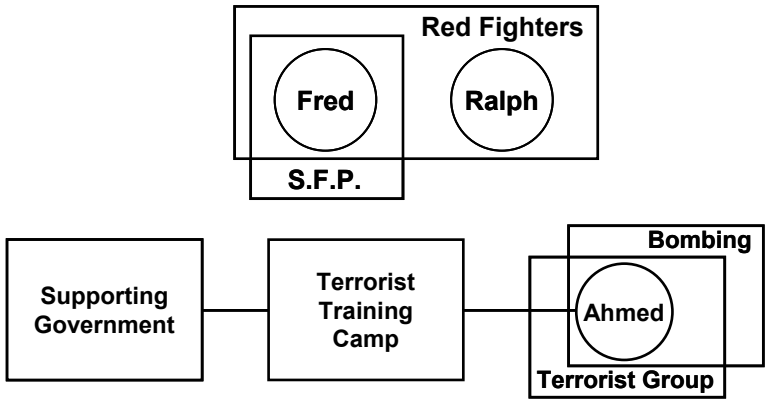
- Each person or non-personal entity is depicted only once in a link analysis diagram.

12-27. The following diagram shows only connectivity between persons:



12-28. The analyst can easily determine from the diagram that Alpha knows Bravo, Bravo knows Charlie and Delta. Bravo is suspected of knowing Echo and Charlie knows Delta, Bravo, and Echo. Although the same information could be shown on a matrix, it is easier to understand when depicted on a link analysis diagram. As situations or investigations become more complex, the ease in understanding a link analysis diagram becomes more apparent. In almost all cases, the available information is first depicted and analyzed on both types of matrices, which are then used to construct a link analysis diagram for further analysis.

12-29. Link analysis diagrams can show organizations, membership within the organization, action teams or cells, or participants in an event. Since each individual depicted on a link analysis diagram can be shown only once, and some individuals may belong to more than one organization or take part in more than one event, squares or rectangles representing non-personal entities may have to overlap. The following illustration demonstrates that Ralph and Fred are both members of the "Red Fighters," and that Fred also is a member of the "Students for Peace." Further, since Ralph and Fred are shown in the same “box,” it is a given that they are mutually associated.



12-30. There is more to overlapping organizations than is immediately obvious. At first glance, the overlap indicates only that an individual may belong to more than one organization or has taken part in multiple activities. Further study and analysis would reveal connections between organizations, connections between events, or connections between organizations and events, either directly or through persons. The above diagram reveals a more

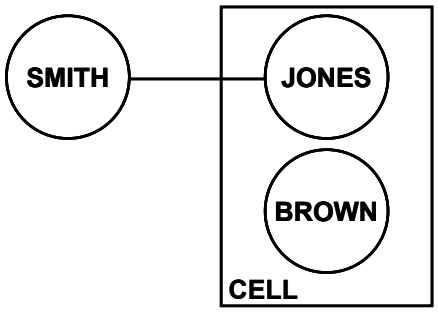
complex connection between organizations, personal connections, and linkages.

12-31. The analysis diagram in paragraph 12-29 shows a connection between organizations and events to which an individual belongs or is associated. In this case, a national government runs a training camp for terrorists. Ahmed, a member of the terrorist group, is associated with the training camp, and participated in the bombing attack. From this diagram, one can link the supporting government to the bombing through the camp and the participant.

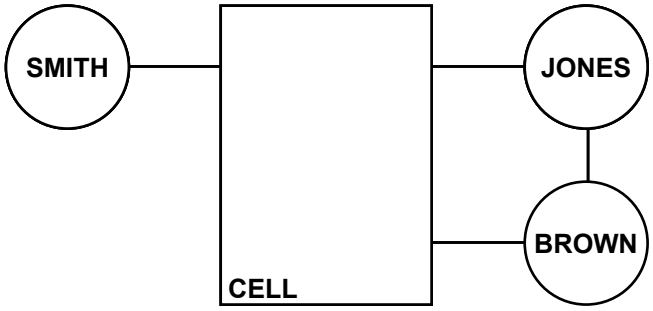
12-32. When, as is often the case, an organization or incident depicted in a link analysis diagram contains the names of more than one individual, it is not necessary to draw a solid line between those individuals to indicate connectivity. It is assumed that individual members of the same cell or participants in the same activity know each other, and the connection between them is therefore implied. If the persons are **not** mutually associated, they cannot be placed in the same "box." Another solution must be found to depict the situation; that is, show the persons as associated with a subordinate or different organization or activity.

12-33. A final set of rules for link analysis diagrams concerns connectivity between individuals who are not members of an organization or participants in an activity, but who are somehow connected to that entity. Two possibilities exist: First, the individual knows a member or members of the organization but is not associated with the organization itself; or second, the person is somehow connected with the organization or activity but cannot be directly linked with any particular member of that entity.

12-34. In the first case, the connectivity line is drawn only between the persons concerned as depicted here:



12-35. In the second case, where Smith is associated with the entity, but not the persons who are members of entity, the situation is shown as depicted here:

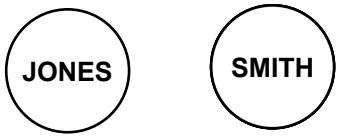


12-36. The steps in constructing a link analysis diagram are as follows:

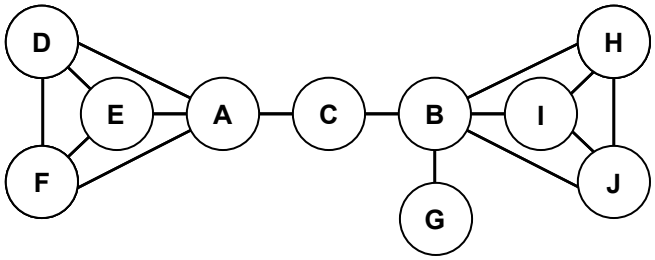
- **Step 1**. Raw data or fragments of information are organized into logical order. Names of individuals, organizations, events, and locations are compiled on appropriate lists. At this point, a time event chart may be completed to assist in understanding the information and to arrange events into chronological order.
- **Step 2**. Information is entered onto the appropriate matrices, graphically displaying "who is associated with whom" and "who is associated with what."
- **Step 3.** Drawing information from the database and intelligence reports, and relationships from the matrices, the link analysis diagram can be constructed. The best method to start the link analysis diagram is to—
 - Start with the association matrix and determine which person has the greatest number of personal associations. Depict that person in the center of the page.



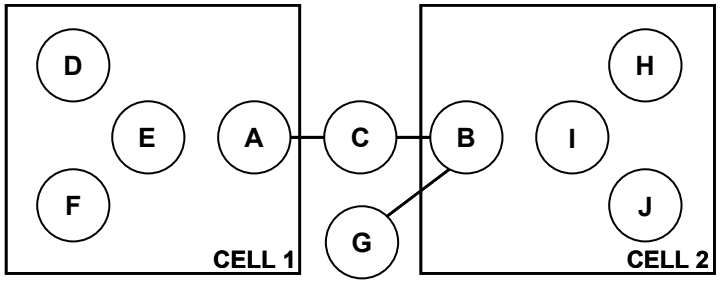
 - Determine which person has the next highest number of personal associations. Depict that person near the first person.



12-37. Use the association matrix and show all confirmed and suspected personal associations.



- After all personal associations have been shown on the link analysis diagram, the analyst uses the activities matrix to determine which activities, organizations, or other non-personal entities need to be depicted by appropriate rectangles. Having done so, the lines of connectivity between persons within the rectangles may be removed to prevent clutter. (It is assumed that participants in the same activity or members of the same cell are acquainted.)



12-38. As shown in Figure 12-4, the link analysis diagram depicts the membership, organization, activities, and connections of the group that, under the leadership of Sheik Omar Abdul Rahman, carried out the bombing of the World Trade Center in New York City and planned other bombing attacks. Together with the time event chart (Figure 12-1), one can gain a basic understanding of the group and its activities, and develop working hypotheses for additional collection and analysis efforts.

12-39. After completion of the matrices and the link analysis diagram, the analyst makes recommendations about the group's structure, and areas can be identified for further collection. Collection assets are employed to verify suspected connections, ID key personalities, and substantiate or refute the conclusions and assessments drawn from the link analysis that has been done. The link analysis diagram and thorough analysis of the information it contains can reveal a great deal about an organization. It can identify the group's leadership, its strong and weak points, and operational patterns. The analyst can use these to predict future activities.

OTHER ANALYSIS TOOLS

12-40. Pattern analysis is the process of deducing the doctrine and TTP that threat forces prefer to employ by careful observation and evaluation of patterns in its activities. This technique is based on the premise that threat COAs reflect certain characteristic patterns that can be identified and interpreted. Pattern analysis can be critically important when facing a threat whose doctrine is unknown and it is necessary to create new threat model and doctrinal templates. Three additional tools that can help the analyst to determine operational patterns and create and update their threat model are the coordinates register, pattern analysis plot sheet, and OB factors.

Coordinates Register

12-41. The coordinates register, or incident map, is one type of pattern analysis tool (Figure 12-5). It illustrates cumulative events that have occurred within the AO and focuses on the "where" of an event. The analyst may use multiple coordinates registers that focus on a different subject or blend subjects. Normally, the coordinates register includes additional information such as notes or graphics. The analyst should use the coordinates register in conjunction with the pattern analysis plot sheet.

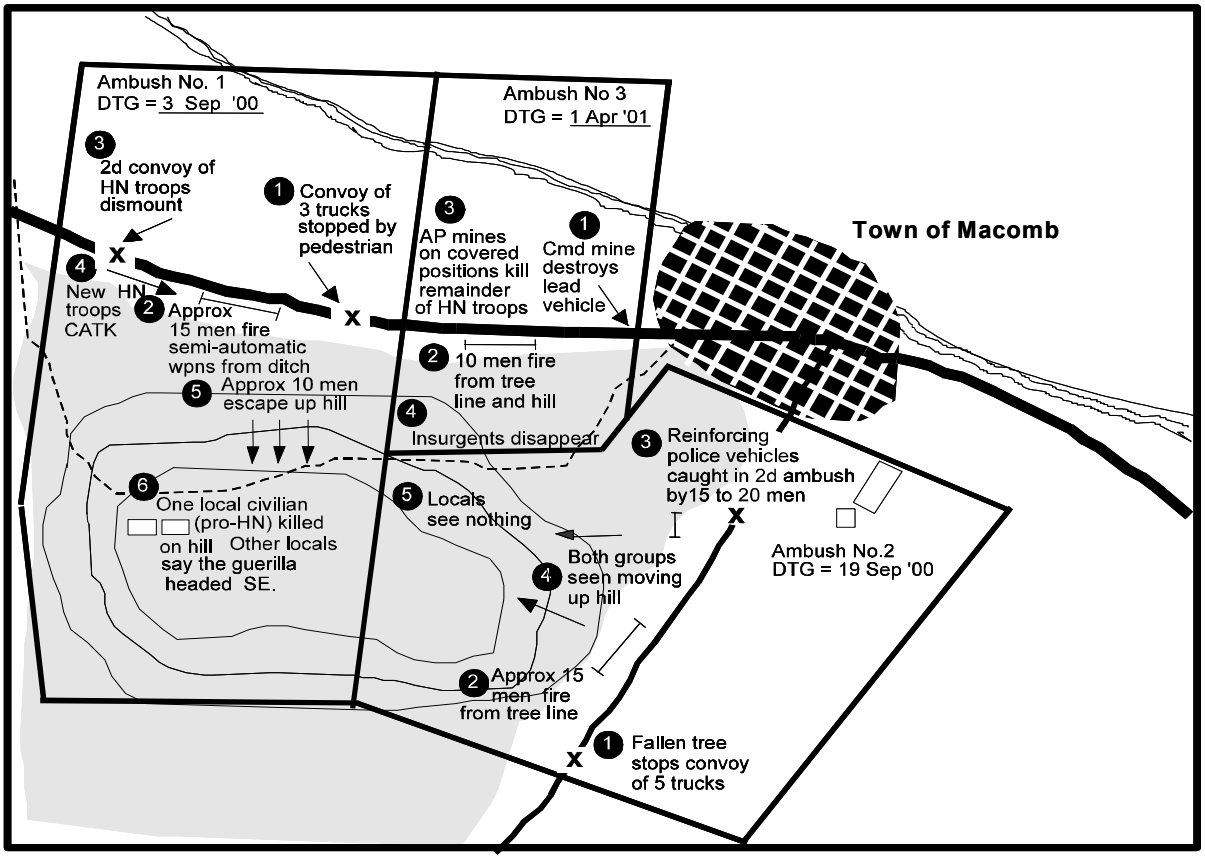


Figure 12-5. Coordinates Register.

Pattern Analysis Plot Sheet

12-42. The analyst uses a pattern analysis plot sheet to focus on the time and date of each serious incident that takes place within the AO (Figure 12-6) The rings depict days of the month; the segments depict the hours of the day As shown in the sheet's legend, the event itself is identified by using an alphanumeric designation and directly corresponds to the legend used on the coordinates register. Another type of the pattern analysis plot sheet helps distinguish patterns in activities that are tied to particular days, dates, or times. When used in conjunction with the coordinates register and any doctrinal templates, a pattern analysis plot sheet supplies the bulk of the data needed to complete an event template.

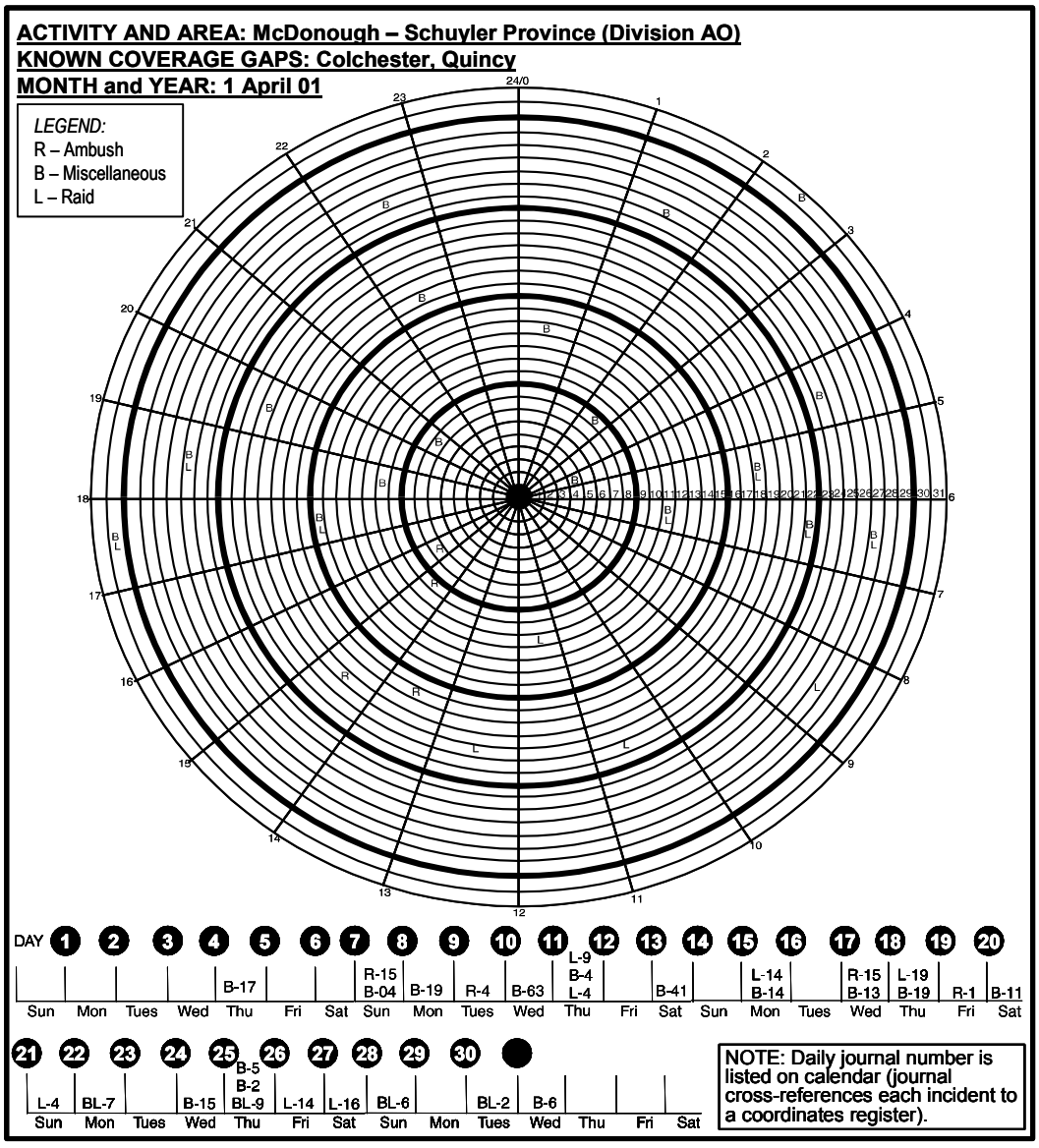


Figure 12-6. Pattern Analysis Plot Sheet.

OB Factors

12-43. A final analytical tool is OB. The OB does not predict enemy intentions or probable COAs but is a means of cataloging intelligence data that qualifies and quantifies certain aspects of threat units. The analyst uses nine factors shown in Table 12-1 to focus the analysis. These help the analyst determine threat capabilities, vulnerabilities, and COAs. Although the situation may dictate that one or more of the factors are given a higher priority, generally speaking, they are all of equal importance. The OB framework, while initially developed to support force-on-force offensive and defensive operations, is easily adapted to support stability and reconstruction operations and to depict "unconventional" forces or even civilian organizations.

Table 12-1. Order of Battle Factors.

Factor	Component
Composition	• Unit identification • Organization
Disposition	• Geographical Location • Tactical Deployment • Movements
Strength	• Personnel • Weapons and Equipment • Types of Units
Tactics	• Tactical Doctrine • Special Operations
Training	• Individual • Unit • Specialized
Logistics	• Systems • Status • Funding
Combat Effectiveness	• Combat Experience • Morale • Tactics • Logistics
Electronic Technical Data/Emitter Nomenclature	• Emitter Type • Mode of Emission • Frequency Range • Location Accuracy for Direction Finding • Associated Use (Units or Weapons)
Miscellaneous	• Personalities/Leadership • Unit History • Uniforms and Insignia • Code Names and Numbers

12-44. The OB is based on the premise that there are certain constants to any group activity. All groups whether they are conventional military forces, insurgent groups, or civilian organizations must have an organizational structure (composition). This structure may not be easily discernable but it will exist. Likewise, any organization has a location or locations in which it operates, personnel and equipment numbers, a system for training, getting supplies, judging efficiency and effectiveness of its operations, communi-

cating, and taking care of other intangibles such as morale. The OB gives the analyst a framework to organize information. The analyst adapts the topic headings to match the particular environment.

HUMINT SOURCE SELECTION

12-45. HUMINT source selection involves identifying, researching, and actively locating a specific group, organization, or individual for the purpose of collecting information in response to intelligence requirements. The HUMINT source selection process includes the C/J/G/S2X, the HOC, the HAT, the OMT, and the HCT. The source selection process allows the HUMINT team leader to identify the most likely source of information, eliminating the uncertainty of the access and placement of sources. Source selection also helps optimize the HUMINT collection effort. Any individual, group, organization, or agency that can be approached for information regarding intelligence requirements is a potential source. Sources are chosen according to their reliability, level of cooperation, and placement and access. Selection is particularly important in stability and reconstruction operations where the HUMINT collectors have access to a large potential source pool. Source selection establishes which current sources can best answer requirements and establishes source profiles to support the screening and selection of new sources.

ESTABLISH DATABASES AND TARGET FOLDERS

12-46. The establishment of local databases, target folders, and personality files is normally the responsibility of the OMT. This is done in coordination with the supporting ACE or analysis control team (ACT). Databases are required to manage the information. By using databases one can identify gaps in the information. The HCT and OMT access higher databases through intelligence reach to share and deconflict locally maintained data with higher level databases. Local databases can be created and used to help track source production, knowledge, reliability, and accuracy, and they simplify cross-reference data that is of primarily local interest. It is ideal to review and update databases at least weekly.

12-47. A target folder provides the collector with up-to-date intelligence information about details of the target. It includes anything of HUMINT value including biographies, descriptions, photographs, and previous information reports. The information can be gained from the ACE or ACT, past reports, INTSUMs, and databases; it can then be organized into easily accessible automated folders. Information on people is categorized and recorded in a personality file. The file serves as reference material for collectors. Information on key military and civilian figures can be of significant value when establishing unit or group identification, tactics, and combat effectiveness. The file should not only provide information on cultural, religious, tribal, political, military, criminal, and governmental background but also contain specific personalities for collectors to focus their collection effort on. This allows the collectors to concentrate on mission planning and to conduct their mission rather than to research information.

COMPARE SOURCE LIST WITH REQUIREMENTS

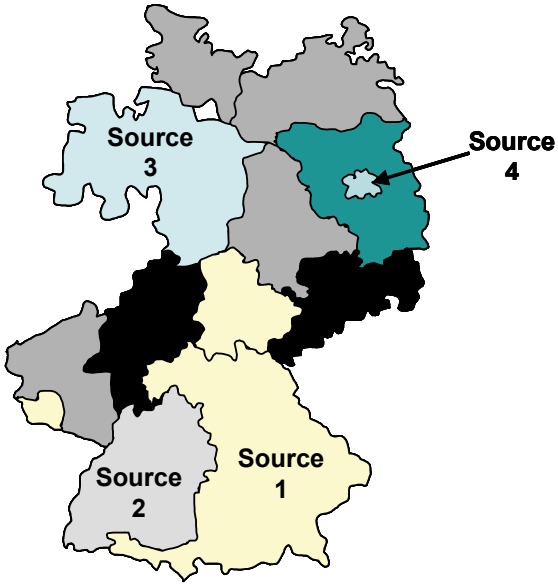
12-48. As target folders are compiled, a list of high-value sources will emerge. It is a simple matter to compare the source list with the PIRs and/or SIRs. This will lead to efficient and time-saving missions for the collectors. Rather than spend time meeting with sources who may have information concerning certain subjects, the HCT is able to tackle the collection process with foresight. Upon receipt of the mission, the OMT conducts mission analysis to determine the optimal way to meet mission requirements. Proper mission analysis enables the collector to properly focus his assets (sources) to gain the maximum amount of intelligence from those sources most likely to possess the highest quality information.

12-49. The following products, which will focus the HCT's collection efforts, can be prepared in conjunction with the ACE and joint intelligence centers:

- Time event charts.
- Source coverage overlays or matrices (see Figure 12-7).
- Link analysis diagrams.
- HUMINT portions of OPORDs and situation reports.

12-50. The source coverage overlay or matrix helps tie in the source coverage to the requirements. It also helps identify gaps in collection. A collection matrix serves the same purpose. It supplies a quick reference when answering intelligence requirements. The matrices must cover both the geographical area and the placement and access of the source. A demographic overlay helps to identify ethnic groups in an area and to track events and patterns based on religious or ethnic differences. The overlay and matrix are examples of how source coverage can be tied to intelligence requirements.

12-51. Source profiles are vital to screening sources for HUMINT collection operations and to identifying personnel that might be of interest to other agencies such as CI and TECHINT. As the situation changes, the HCT might be tasked with new collection requirements that cannot be answered by the current sources. The HCT is constantly looking for new and better sources. When presented with new requirements, the OMT develops a source profile of the type of individual that would most likely be able to provide the information required. This profiling can include placement, access, age, ethnic type, gender, location, occupation, and military specialty. The OMT first searches through existing local databases to try to get a source match. If not, it passes the profile to the HCTs along with the requirements to facilitate their screening of potential sources.



		L AREA	PIR 1	PIR 2	PIR 3	PIR 4	PIR 5	PIR 6
0001	Police	Village 1	X					
0002	Municipal Government	Village 1 and National		X	X			
0003	Political Party 1	City 1 and 2			X		X	
0004	Political Party 2	City 3 and 4		X		X		X

Figure 12-7. Example of a Source Coverage Overlay or Matrix.

This page intentionally left blank.

Chapter 13

Automation and Communication

13-1. Modern automation and communications systems are vital to HUMINT collection. Real-time collaboration, detailed operational planning and ISR integration, as well as enhanced collection and source exploitation tools, must support team efforts. Emerging technology continues to allow the entire HUMINT collection system to operate more effectively. Commanders must be prepared to supply their HUMINT collection assets with the best possible technology not only to enhance collection but also to optimize the survivability of the collectors. (See Appendix L.) Commanders may not be able to rely solely on standard military equipment but must be prepared to bridge the inevitable technological development gap through the identification and adaptation of commercially available products and technologies. For specific system components and capabilities, see ST 2-50.

AUTOMATION

13-2. HUMINT automation uses common hardware and software solutions with a flexible interactive user interface to provide standardization of equipment and processes across all operational environments and conditions. HUMINT automation must be deployable and scalable to fit the mission or force package. System components must be capable of intelligence reach to support forward-deployed elements. HUMINT automation allows integration and interaction with existing intelligence operations, HUMINT operational systems, and databases. This integration allows operations personnel and analysts to develop plans and levy collection and operational requirements, as well as to manage, control, analyze, and report the information collected. HUMINT automation—

- Provides connectivity and reach capability between all echelons of HUMINT activity.
- Receives higher echelon requirements and transmits requests for information.
- Converts HUMINT reporting into formats for JTF or coalition task force (CTF), theater, or national consumption.
- Pushes requirements, requests, and plans for HUMINT operations in theater as required.
- Maintains the central HUMINT database for the theater or AO.
- Leverages JTF or CTF, theater, and national level requirements and products for strategic, operational, and tactical HUMINT assets in theater.

- Enables HUMINT to provide accurate and timely correlated information to supported commanders through established reporting channels.
- Provides automated analysis tools.

13-3. Systems such as Trusted Workstation (TWS) can convert HUMINT reporting into formats for JTF or CTF, theater, or national consumption. TWS can also connect between the SIPRNET and any lower level networks, such as coalition, multinational, or NATO, or unclassified networks such as NIPRNET or the Internet.

COLLECTION SUPPORT AUTOMATION REQUIREMENTS

BIOMETRICS

13-4. Biometrics is the study of measurable biological characteristics. In HUMINT collection, biometric devices, usually computer based, enable the HUMINT collector to use biological data to support the collection and analysis effort. Biometrics can also be used in non-HUMINT efforts to collect and maintain evidence for criminal prosecution. The two major types of biometric data that are useful to the HUMINT collector are identification data and data that indicate source truthfulness. Identification devices use biological information such as fingerprints, voiceprints, facial scans, and retinal scans to match an individual to a source database. They can verify the identity of a specific individual from the target population during screening.

13-5. HCTs may be equipped with portable equipment for collecting, storing, analyzing, forwarding, and retrieving biometric information. The BAT is able to identify personnel by using identifying characteristics of their irises, fingerprints, or facial photograph. The structured query language (SQL) server-based database links identifying characteristics with all previous reports related to the person. Once a person's identifying characteristics are entered into the database, if that person is again detained and scanned, the system has a probability of identifying them that approaches 100 percent. This ability is especially useful for determining if a source is providing the same information to multiple collectors; thereby avoiding false confirmation of information. HUMINT collectors primarily use BAT during screening operations at all echelons; from checkpoint screening, to screening at a DCP, to screening at a JIDC. MPs use the Detainee Reporting System (DRS) during in-processing at internment facilities. The DRS records data for detainee processing and tracking and is intended to interact with the BAT system to avoid duplication of effort.

13-6. The hardware that makes up the system, which is given to MI teams, consists of a commercial off-the-shelf (COTS) semi-hardened laptop computer running an operating system with a graphical user interface. It has a camera and an iris scanner, each of which is portable and can be used independent of the computer to collect and temporarily store information. The system also includes a fingerprint scanner that conforms to FBI requirements for admissible evidence. The fingerprint scanner must be attached to the computer during use.

13-7. Biometric devices such as voice stress analyzer and polygraph support the determination of the truthfulness of a source. The polygraph is of limited usefulness in general HUMINT collection due to the level of expertise needed to operate it and the lack of general availability of the device to the field. As devices are developed that can remotely collect and report information to the HUMINT collector on subtle changes in the source's respiration, heartbeat, perspiration, and eye movement that can be indicators of deceit, they can be used to support HUMINT collection.

MACHINE TRANSLATION AND INTERPRETATION

13-8. Understanding oral and written communication in a foreign language is often the center of effective HUMINT collection operations. The optimal solution is to have an individual who is a trained collector of native proficiency, totally versed in the local situation and US requirements, with the requisite security clearance, who is capable of reporting accurately in English. Commanders' access to such individuals is usually problematic. This requirement is met through a combination of MI linguists, contractors, native speakers within the DOD system, and locally hired civilian translators. Difficulties arise if the proficiency levels of MI linguists are not up to mission requirements, or if the linguists do not possess the proper language for the theater of operation. Using locally hired translators raises security problems. In light of these conditions, an increasingly viable solution for the commander is the use of machine translation devices to meet some of these requirements.

13-9. Voice and text translation machines or software are critical in augmenting available linguists. This includes natural language processing, artificial intelligence, and optical character recognition (OCR) capabilities. The basic application of machine translation, such as speech recognition and OCRs, dramatically increases the speed of processing information. Software programs are becoming widely available that allow a non-linguist to determine the intelligence significance of a foreign document, aid linguists with laborious tasks, and add consistency to human translation.

13-10. Machine interpretation is the use of a machine to interpret the spoken word between the HUMINT collectors and another individual speaking a foreign language. Linguists are in high demand during operations and usually limited in number. As machine interpretation devices that address this problem become available to the field, they will improve the communication ability of non-linguists.

ANALYTICAL AUTOMATION REQUIREMENTS

13-11. The requirement for a robust HUMINT single-discipline analytical capability extends through all echelons from national level to the OMTs. Communication between HUMINT analysts at the operational level and analysts at the staff level may best be accomplished through a web-based communication capability. Web-based visual analytical tools allow maximum analyst participation in the development of products geared to mission planning, targeting, and information analysis at all echelons.

Analytical products must be responsive to the special needs of a specific collection operation, project, or element.

13-12. HUMINT collectors run operations in terrain made up of persons, organizations, and installations of interest. Intelligence analysis support determines the specific terrain in each team area and how it differs from one team's named area of interest (NAI) to another. Specific products include studies on nominated targets (persons, organizations, and installations) and trends based on HUMINT reporting, as appropriate, and visual analysis products (time event charts, matrices, link analysis diagrams, and organizational diagrams).

AUTOMATED ANALYSIS TOOLS

13-13. Automation of HUMINT analytical tools such as time event charts, association matrices, activity matrices, and link analysis diagrams dramatically increase predictive analysis capability. Automation saves time and permits access to more complete information thus producing a more accurate, timely product. Automated analysis techniques, aided by computerized virtual-viewing programs, allow the analyst better battlefield visualization. Automated analysis, linked to data and databases, includes artificial intelligence programs. These programs assist the analyst in developing predictions and identifying information gaps to support targeting and collection. Automation and web-based tools allow the analyst to—

- Track and cross-cue HUMINT reports.
- Incorporate data extraction technology, retrieval, automated data organization, content analysis, and visualization.
- Share analytical conclusions with HUMINT teams and other analysts in real time.
- Apply multidimensional technologies, content analysis techniques, and web-based collaborations.
- Display analytical results and view HUMINT operations in real time.
- Share resources such as models, queries, visualizations, map overlays, geospatial images, and tool outputs through a common interface.
- Apply clustering (a nonlinear search that compiles the results based on search parameters) and rapid spatial graphical and geographic visualization tools to determine the meaning of large informational streams.
- Rapidly discover links, patterns, relationships, and trends in text to use in predictive analysis.
- Capture analytical conclusions and automatically transfer to intelligence databases and systems.

SEARCH ENGINES

13-14. Search engines provide access to previously collected or known information facilitating the development of comprehensive analytical and intelligence products and avoiding unnecessary collection tasking redundancy. A tool set for data visualization, search, and discovery is required, which is embedded with several software programs for manipulating data from multiple databases. The types of modules in visualization packages should include search engines and knowledge discovery (semantic clustering) for unformatted data, applications for extracting and organizing formatted data, and data labeling. The package should also include a model building tool to enable users to make their archives more efficient with respect to search, retrieval, and compatibility to other applications as well as archiving and maintenance tools to support what will eventually become a large data warehouse. Search engines should be—

- Multilingual and able to query multiple classified and unclassified databases.
- Capable of developing, querying, and manipulating stored information.

WEB-BASED REPORTING AND PORTALS

13-15. Web-based reporting employs current Internet portal technology. The web-based portal is an efficient and effective means of developing a repository of HUMINT information. It employs an interactive graphic interface using client browser technology, search engines, hyperlinks, and intelligent software agents for searching, finding, viewing, and maintaining databases and supporting HUMINT work, data, and information flows. It supports collaborative analysis at multiple echelons through connectivity on the SIPRNET. The following pertains to web-based reporting:

- Web-based databases work with any computer hardware, operating system, or software and can be made accessible through web portals.
- Firewalls and information access are controlled at each level with an approving systems administrator at each level conducting quality control through release authority procedures.
- Graphic user interface uses standard Army and DOD report formats.
- Graphic user interface walks the user through a critical task and is able to identify Army and DOD reports as required. Reports must be Army and DOD platform compatible and transferable through and to their respective systems.
- Multimedia supports applications for attaching, associating, and hyperlinking video, still photographs, voice, scanned objects, graphics, and maps to records and files.

13-16. Web-based reporting and web pages developed for specific products allow the user to—

- Leverage their effort and expertise against all requirements, not just the ones that must be met immediately.

- Identify timely intelligence gaps and the leads to fill those gaps.
- Ensure immediate analytical feedback on collector reports to—
 - Post questions directly to a web page to enable all HCTs to answer or be cued to the specific request.
 - Identify or request clarification on questionable data for quality control.
- Fuse HUMINT information and all-source information as required.
- Focus collection teams supporting maneuver commanders' requirements more effectively.
- Immediately extract information for crisis reaction.

13-17. If HCTs use web portals to submit reports directly to theater level, they must also send the reports through their OMT for submission to the 2X. Failure to do so may deny the 2X the ability to deconflict and cross-reference reports. HUMINT collectors must ensure that they follow the theater-specific methodology for access to the theater web portal.

DATABASES

13-18. Without databases, information is difficult or impossible to retrieve quickly, especially under adverse conditions. Databases allow access to data in a distributed environment and support many complex HUMINT functions and requirements, including—

- Mission deconfliction.
- RM.
- RFIs.
- HUMINT analysis.
- Summary, report, and assessment preparation.
- Threat and friendly situation tracking.
- Targeting.

13-19. Databases interact with other tools to support predictive analysis, prepare graphic analytical products, and provide situational understanding down to the HCT. These databases—

- Support time event charts, association matrices, link analysis, and other analysis tools.
- Require a designated systems administrator at each. To ensure a high degree of integrity, discrepancies must be verified for accuracy.
- Allow operators, managers, and analysts to—
 - Compartment (protect) source-sensitive operational database segments, files, records, and fields.
 - Create, update, and maintain databases from locally generated information.
 - Import complete or partial databases from larger or peer databases.
 - Export complete or partial databases to peer or larger databases.

 - Share data and databases between peers, subordinates, or higher with appropriate access authorization.
- Provide systematic processing and automated parsing using standardized forms in intelligence operations, which are automatically parsed into appropriate databases for information storing, sharing, retrieval, and analysis.
- Allow query functions for decisionmaking as well as operational and analytical support.
- Provide analytical programs able to correlate data that facilitate information retrieval from any data repository.
- Incorporate information retrieval functions such as browsing (that is, point and click), key word searching, concepts, and similar functions.
- Support a suite of specialized decision support software (DSS)—a set of tools which supports HUMINT source administration, analysis, and risk management decisions. DSS tools should produce a set of HUMINT reports specifically tailored to the HUMINT decisionmaking, analysis, and assessment process.

13-20. HARMONY is the national intelligence database for foreign DOCEX and translations management. HARMONY is the single, comprehensive bibliographic reference for all available primary source foreign technical and military documents and their translations. This single database concept eliminates duplicate collection, translation, and reporting of primary source foreign technical and military documents and greatly streamlines the process of providing exploited documents to consumers. The HARMONY database application uses the DOD Information Infrastructure (DII) Common Operating Environment (COE) guidance. The HARMONY database is web-enabled and can be readily accessed, easily used, and responsive to the needs of analysts and other consumers within the US Government community.

AUTOMATION SYSTEMS

13-21. The HUMINT collection automation systems are normally shared systems used by both the HUMINT and CI communities. They must have connectivity with lateral units as well as higher and subordinate elements.

C/J/G/S2X, HOC, AND HAT AUTOMATION REQUIREMENTS

13-22. The HUMINT staff elements need to receive input from the OMTs and HCTs as well as input from higher and lateral echelons. They must be able to conduct HUMINT planning, RM, and report dissemination. They must transmit technical support information, interface with ACE and automated analysis systems, manipulate HUMINT databases, conduct reach, and have access to HUMINT analytical tools.

OMT AND COLLECTION TEAM LEADER REQUIREMENTS

13-23. The OMT must be able to track teams and team members; receive and transmit data including graphic data to and from higher, lateral, and lower HUMINT elements; create, receive, edit, and transmit reports; conduct single-discipline HUMINT analysis; receive and transmit technical support information and tasking information; conduct reach; and conduct mission planning.

INDIVIDUAL COLLECTOR AUTOMATION REQUIREMENTS

13-24. The key to effective HUMINT collection is unimpeded communication between the collector and the source of information. Any technological support to HUMINT collection must be as unobtrusive as possible to minimize the intimidation factor when dealing with human sources. The individual collector must be able to—

- Record (both video and voice) conversations with sources.
- Scan, translate, and transmit documents and photographs.
- Instantaneously locate themselves in both rural and urban environments.
- Immediately access local, theater, and even national level databases.
- Communicate instantaneously with other team elements.

HUMINT AND CI WORKSTATION REQUIREMENTS

13-25. The CI and HUMINT teams have organic computer and data processing equipment. These workstations provide HUMINT and CI teams with both productivity and management and analysis tools. They also provide SIPRNET connectivity and processing capability to identify requirements and facilitate reporting into other DOD systems as required. The HUMINT and CI workstation is able to use standard Army, DOD, and HUMINT and CI reporting programs, standard symbols, programs to produce map overlays, and map plotting software; all of which are included.

13-26. Teams use workstations to—

- Provide quality control and dissemination of reports from the subordinate HCTs.
- Direct activities of subordinate HCTs and provide management to them.
- Perform single-discipline HUMINT analysis for the supported commander.
- Transmit intelligence and administrative reports in NRT to higher headquarters.
- Receive tasking and administrative reports from higher headquarters and distribute to HCTs as required.
- Consolidate local databases and provide database input to higher headquarters.
- Receive database and digital information from higher headquarters and pass to lower and vice versa.

COMMUNICATIONS

13-27. Successful HUMINT operations must be supported by multi-echelon technical control and a communications system that provides internal team communications, links HCTs to OMTs, and links OMTs to higher headquarters, analytical elements, and theater and national agencies.

COMMUNICATION ARCHITECTURE

13-28. The HUMINT collection architecture requires operation on several communications and processing nets. These nets provide the framework needed to coordinate the tasking, reporting, C2, and service support of HUMINT collection units spread across the width and depth of the battlefield. Under most operational scenarios, HCTs are not stationary. They are constantly moving throughout their supported command's AO and are able to communicate on the move. They cannot rely on fixed communications nodes for support. Communications redundancy ensures the loss of any one system does not severely disrupt HUMINT operations. HCTs and OMTs normally operate at the collateral security level to ensure the timely dissemination of combat information and targeting data to organizations operating outside MI channels. The C/J/G/S2X normally requires access to Top Secret (SCI) communications capabilities to maintain coordination with national level agencies.

13-29. The HUMINT collection assets use three basic communications nets: the operations and intelligence (O/I) net, a command net, and a HUMINT-specific technical net. Dependent on their mission and battlefield location, the HCTs may also need to monitor the fire support element (FSE), aviation, or air defense artillery (ADA) communications nets.

- The O/I net links the collectors and producers of intelligence to the consumers of the intelligence information. It is used to pass information of immediate value to the affected unit and to analytical elements at the supported unit.
- The command nets exist at every echelon of command. They link the superior headquarters with its subordinate elements. Normally a unit will operate on two command nets; the one that links that unit to its higher headquarters and the one that links that unit to its subordinate elements. HUMINT elements will also use their unit's command net to coordinate logistic and administrative support.
- The technical nets link the control team to all of their subordinate collection teams and to the centers or organizations that provide the databases and technical guidance necessary for single-discipline collection and analysis. For example, the technical net would connect HCTs through their control teams to the S2X and higher echelon HUMINT analysis organizations.

MOBILE COMMUNICATIONS REQUIREMENTS

13-30. HUMINT mobile communications requirements augment the network connectivity that elements should have when at a base camp or facility; they vary with each element's mission and location as follows:

- Individual HUMINT collectors must maintain communications capability with the other team members and the team leader while dismounted. HUMINT collectors, especially when supporting offensive and defensive operations, may be deployed as individuals. They need to maintain contact with their team leader for technical and operational support.
- The HCT may operate anywhere within the supported unit's AO. They may operate mounted or dismounted. If supporting airmobile, airborne, amphibious, or other mobile operations, they may not have access to their vehicle-mounted communications systems for the critical early stages of these operations. They receive and report operational and technical information, as well as report intelligence information to the OMT using their unit's command net. They monitor their superior unit's O/I net. If in DS to a maneuver element, they also monitor the command net of the unit they are supporting.
- OMTs normally operate on the superior unit O/I net, their unit C2 net, and the HUMINT technical net. If the OMT is in DS, it must also operate on the C2 net of the supported unit.
- The C/J/G/S2X operates on the C2 net, monitors the O/I net, and controls its echelon HUMINT technical net. The 2X needs secure (SCI) communications capability to coordinate operations and pass data between themselves and higher HUMINT organizations.

Appendix A

Geneva Conventions

SECTION I. GENEVA CONVENTIONS RELATIVE TO THE TREATMENT OF PRISONERS OF WAR (THIRD GENEVA CONVENTION)

The articles in this section are extracted from the Geneva Convention Relative to the Treatment of Prisoners of War, 12 August 1949.

PART I GENERAL PROVISIONS

ARTICLE 1

The High Contracting Parties undertake to respect and to ensure respect for the present Convention in all circumstances.

ARTICLE 2

In addition to the provisions which shall be implemented in peace time, the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them.

The Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance.

Although one of the Powers in conflict may not be a party to the present Convention, the Powers who are parties thereto shall remain bound by it in their mutual relations. They shall furthermore be bound by the Convention in relation to the said Power, if the latter accepts and applies the provisions thereof.

ARTICLE 3

In the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties, each party to the conflict shall be bound to apply, as a minimum, the following provisions:

1. Persons taking no active part in the hostilities, including members of armed forces who have laid down their arms and those placed hors de combat by sickness, wounds, detention, or any other cause, shall in all circumstances be treated humanely, without any adverse distinction founded on race, color, religion or faith, sex, birth or wealth, or any other similar criteria. To this end the following acts are and shall remain prohibited at any time and in any place whatsoever with respect to the above-mentioned persons:

(a) Violence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture;

(b) Taking of hostages;

(c) Outrages upon personal dignity, in particular, humiliating and degrading treatment;

(d) The passing of sentences and the carrying out of executions without previous judgment pronounced by a regularly constituted court affording all the judicial guarantees which are recognized as indispensable by civilized peoples.

2. The wounded and sick shall be collected and cared for.

An impartial humanitarian body, such as the International Committee of the Red Cross, may offer its services to the Parties to the conflict.

The Parties to the conflict should further endeavor to bring into force, by means of special agreements, all or part of the other provisions of the present Convention.

The application of the preceding provisions shall not affect the legal status of the Parties to the conflict.

ARTICLE 4

A. Prisoners of war, in the sense of the present Convention, are persons belonging to one of the following categories, who have fallen into the power of the enemy:

1. Members of the armed forces of a Party to the conflict as well as members of militias or volunteer corps forming part of such armed forces.

2. Members of other militias and members of other volunteer corps, including those of organized resistance movements, belonging to a Party to the conflict and operating in or outside their own territory, even if this territory is occupied, provided that such militias or volunteer corps, including such organized resistance movements, fulfill the following conditions:

(a) That of being commanded by a person responsible for his subordinates;

(b) That of having a fixed distinctive sign recognizable at a distance;

(c) That of carrying arms openly;

(d) That of conducting their operations in accordance with the laws and customs of war.

3. Members of regular armed forces who profess allegiance to a government or an authority not recognized by the Detaining Power.

4. Persons who accompany the armed forces without actually being members thereof, such as civilian members of military aircraft crews, war correspondents, supply contractors, members of labor units or of services responsible for the welfare of the armed forces, provided that they have received authorization from the armed forces which they accompany, who shall provide them for that purpose with an identity card similar to the annexed model.

5. Members of crews, including masters, pilots and apprentices, of the merchant marine and the crews of civil aircraft of the Parties to the conflict, who do not benefit by more favorable treatment under any other provisions of international law.

6. Inhabitants of a non-occupied territory, who on the approach of the enemy spontaneously take up arms to resist the invading forces, without having had time to form themselves into regular armed units, provided they carry arms openly and respect the laws and customs of war.

B. The following shall likewise be treated as prisoners of war under the present Convention:

1. Persons belonging, or having belonged, to the armed forces of the occupied country, if the occupying Power considers it necessary by reason of such allegiance to intern them, even though it has originally liberated them while hostilities were going on outside the territory it occupies, in particular where such persons have made an unsuccessful attempt to rejoin the armed forces to which they belong and which are engaged in combat, or where they fail to comply with a summons made to them with a view to internment.

2. The persons belonging to one of the categories enumerated in the present Article, who have been received by neutral or non-belligerent Powers on their territory and whom these Powers are required to intern under international law, without prejudice to any more favorable treatment which these Powers may choose to give and with the exception of Articles 8, 10, 15, 30, fifth paragraph, 58-67, 92, 126 and, where diplomatic relations exist between the Parties to the conflict and the neutral or non-belligerent Power concerned, those Articles concerning the Protecting Power. Where such diplomatic relations exist, the Parties to a conflict on whom these persons depend shall be allowed to perform towards them the functions of a Protecting Power as provided in the present Convention, without prejudice to the functions which these Parties normally exercise in conformity with diplomatic and consular usage and treaties.

C. This Article shall in no way affect the status of medical personnel and chaplains as provided for in Article 33 of the present Convention.

ARTICLE 5

The present Convention shall apply to the persons referred to in Article 4 from the time they fall into the power of the enemy and until their final release and repatriation.

Should any doubt arise as to whether persons, having committed a belligerent act and having fallen into the hands of the enemy, belong to any of the categories enumerated in Article 4, such persons shall enjoy the protection of the present Convention until such time as their status has been determined by a competent tribunal.

ARTICLE 6

In addition to the agreements expressly provided for in Articles 10, 23, 28, 33, 60, 65, 66, 67, 72, 73, 75, 109, 110, 118, 119, 122 and 132, the High Contracting Parties may conclude other special agreements for all matters concerning which they may deem it suitable to make separate provision. No special agreement shall adversely affect the situation of prisoners of war, as defined by the present Convention, nor restrict the rights which it confers upon them.

Prisoners of war shall continue to have the benefit of such agreements as long as the Convention is applicable to them, except where express provisions to the contrary are contained in the aforesaid or in subsequent agreements, or where more favorable measures have been taken with regard to them by one or other of the Parties to the conflict.

ARTICLE 7

Prisoners of war may in no circumstances renounce in part or in entirety the rights secured to them by the present Convention, and by the special agreements referred to in the foregoing Article, if such there be.

ARTICLE 8

The present Convention shall be applied with the cooperation and under the scrutiny of the Protecting Powers whose duty it is to safeguard the interests of the Parties to the conflict. For this purpose, the Protecting Powers may appoint, apart from their diplomatic or consular staff, delegates from amongst their own nationals or the nationals of other neutral Powers. The said delegates shall be subject to the approval of the Power with which they are to carry out their duties.

The Parties to the conflict shall facilitate to the greatest extent possible the task of the representatives or delegates of the Protecting Powers.

The representatives or delegates of the Protecting Powers shall not in any case exceed their mission under the present Convention. They shall, in particular, take account of the imperative necessities of security of the State wherein they carry out their duties.

ARTICLE 9

The provisions of the present Convention constitute no obstacle to the humanitarian activities which the International Committee of the Red Cross or any other impartial humanitarian organization may, subject to the consent of the Parties to the conflict concerned, undertake for the protection of prisoners of war and for their relief.

ARTICLE 10

The High Contracting Parties may at any time agree to entrust to an organization which offers all guarantees of impartiality and efficacy the duties incumbent on the Protecting Powers by virtue of the present Convention.

When prisoners of war do not benefit or cease to benefit, no matter for what reason, by the activities of a Protecting Power or of an organization provided for in the first paragraph above, the Detaining Power shall request a neutral State, or such an organization, to undertake the functions performed under the present Convention by a Protecting Power designated by the Parties to a conflict.

If protection cannot be arranged accordingly, the Detaining Power shall request or shall accept, subject to the provisions of this Article, the offer of the services of a humanitarian organization, such as the International Committee of the Red Cross, to assume the humanitarian functions performed by Protecting Powers under the present Convention.

Any neutral Power or any organization invited by the Power concerned or offering itself for these purposes, shall be required to act with a sense of responsibility towards the Party to the conflict on which persons protected by the present Convention depend, and shall be required to furnish sufficient assurances that it is in a position to undertake the appropriate functions and to discharge them impartially.

No derogation from the preceding provisions shall be made by special agreements between Powers one of which is restricted, even temporarily, in its freedom to negotiate with the other Power or its allies by reason of military events, more particularly where the whole, or a substantial part, of the territory of the said Power is occupied.

Whenever in the present Convention mention is made of a Protecting Power, such mention applies to substitute organizations in the sense of the present Article.

ARTICLE 11

In cases where they deem it advisable in the interest of protected persons, particularly in cases of disagreement between the Parties to the conflict as to the application or interpretation of the provisions of the present Convention, the Protecting Powers shall lend their good offices with a view to settling the disagreement.

For this purpose, each propose to the Parties of the Protecting Powers may, either at the invitation of one Party or on its own initiative, to the conflict a meeting of their representatives, and in particular of the authorities responsible for prisoners of war, possibly on neutral territory suitably chosen. The Parties to the conflict shall be bound to give effect to the proposals made to them for this purpose. The Protecting Powers may, if necessary, propose for approval by the Parties to the conflict a person belonging to a neutral Power, or delegated by the International Committee of the Red Cross, who shall be invited to take part in such a meeting.

PART II GENERAL PROTECTION OF PRISONERS OF WAR

ARTICLE 12

Prisoners of war are in the hands of the enemy Power, but not of the individuals or military units who have captured them. Irrespective of the individual responsibilities that may exist, the Detaining Power is responsible for the treatment given them.

Prisoners of war may only be transferred by the Detaining Power to a Power which is a party to the Convention and after the Detaining Power has satisfied itself of the willingness and ability of such transferee Power to apply the Convention. When prisoners of war are transferred under such circumstances, responsibility for the application of the Convention rests on the Power accepting them while they are in its custody.

Nevertheless if that Power fails to carry out the provisions of the Convention in any important respect, the Power by whom the prisoners of war were transferred shall, upon being notified by the PROTECTING Power, take effective measures to correct the situation or shall request the return of the prisoners of war. Such requests must be complied with.

ARTICLE 13

Prisoners of war must at all times be humanely treated. Any unlawful act or omission by the Detaining Power causing death or seriously endangering the health of a prisoner of war in its custody is prohibited, and will be regarded as a serious breach of the present Convention. In particular, no prisoner of war may be subjected to physical mutilation or to medical or scientific experiments of any kind which are not justified by the medical, dental or hospital treatment of the prisoner concerned and carried out in his interest.

Likewise, prisoners of war must at all times be protected, particularly against acts of violence or intimidation and against insults and public curiosity.

Measures of reprisal against prisoners of war are prohibited.

ARTICLE 14

Prisoners of war are entitled in all circumstances to respect for their persons and their honor. Women shall be treated with all the regard due to their sex and shall in all cases benefit by treatment as favorable as that granted to men. Prisoners of war shall retain the full civil capacity which they enjoyed at the time of their capture. The Detaining Power may not restrict the exercise, either within or without its own territory, of the rights such capacity confers except in so far as the captivity requires.

ARTICLE 15

The Power detaining prisoners of war shall be bound to provide free of charge for their maintenance and for the medical attention required by their state of health.

ARTICLE 16

Taking into consideration the provisions of the present Convention relating to rank and sex, and subject to any privileged treatment which may be accorded to them by reason of their state of health, age or professional qualifications, all prisoners of war shall be treated alike by the Detaining Power, without any adverse distinction based on race, nationality, religious belief or political opinions, or any other distinction founded on similar criteria.

PART III CAPTIVITY

SECTION I BEGINNING OF CAPTIVITY

ARTICLE 17

Every prisoner of war, when questioned on the subject, is bound to give only his surname, first names and rank, date of birth, and army, regimental, personal or serial number, or failing this, equivalent information. If he willfully infringes this rule, he may render himself liable to a restriction of the privileges accorded to his rank or status.

Each Party to a conflict is required to furnish the persons under its jurisdiction who are liable to become prisoners of war, with an identity card showing the owner's surname, first names, rank, army, regimental, personal or serial number or equivalent information, and date of birth. The

identity card may, furthermore, bear the signature or the fingerprints, or both, of the owner, and may bear, as well, any other information the Party to the conflict may wish to add concerning persons belonging to its armed forces. As far as possible the card shall measure 6.5 x 10 cm. and shall be issued in duplicate. The identity card shall be shown by the prisoner of war upon demand, but may in no case be taken away from him.

No physical or mental torture, nor any other form of coercion, may be inflicted on prisoners of war to secure from them information of any kind whatever. Prisoners of war who refuse to answer may not be threatened, insulted, or exposed to any unpleasant or disadvantageous treatment of any kind.

Prisoners of war who, owing to their physical or mental condition, are unable to state their identity, shall be handed over to the medical service. The identity of such prisoners shall be established by all possible means, subject to the provisions of the preceding paragraph.

The questioning of prisoners of war shall be carried out in a language which they understand.

ARTICLE 18

All effects and articles of personal use, except arms, horses, military equipment and military documents shall remain in the possession of prisoners of war, likewise their metal helmets and gas masks and like articles issued for personal protection. Effects and articles used for their clothing or feeding shall likewise remain in their possession, even if such effects and articles belong to their regulation military equipment.

At no time should prisoners of war be without identity documents. The Detaining Power shall supply such documents to prisoners of war who possess none.

Badges of rank and nationality, decorations and articles having above all a personal or sentimental value may not be taken from prisoners of war.

Sums of money carried by prisoners of war may not be taken away from them except by order of an officer, and after the amount and particulars of the owner have been recorded in a special register and an itemized receipt has been given, legibly inscribed with the name, rank and unit of the person issuing the said receipt. Sums in the currency of the Detaining Power, or which are changed into such currency at the prisoner's request, shall be placed to the credit of the prisoner's account as provided in Article 64.

The Detaining Power may withdraw articles of value from prisoners of war only for reasons of security; when such articles are withdrawn, the procedure laid down for sums of money impounded shall apply.

Such objects, likewise the sums taken away in any currency other than that of the Detaining Power and the conversion of which has not been asked for by the owners, shall be kept in the custody of the Detaining Power and shall be returned in their initial shape to prisoners of war at the end of their captivity.

ARTICLE 19

Prisoners of war shall be evacuated, as soon as possible after their capture, to camps situated in an area far enough from the combat zone for them to be out of danger.

Only those prisoners of war who, owing to wounds or sickness, would run greater risks by being evacuated than by remaining where they are, may be temporarily kept back in a danger zone.

Prisoners of war shall not be unnecessarily exposed to danger while awaiting evacuation from a fighting zone.

ARTICLE 20

The evacuation of prisoners of war shall always be effected humanely and in conditions similar to those for the forces of the Detaining Power in their changes of station.

The Detaining Power shall supply prisoners of war who are being evacuated with sufficient food and potable water, and with the necessary clothing and medical attention. The Detaining Power shall take all suitable precautions to ensure their safety during evacuation, and shall establish as soon as possible a list of the prisoners of war who are evacuated.

If prisoners of war must, during evacuation, pass through transit camps, their stay in such camps shall be as brief as possible.

SECTION II INTERNMENT OF PRISONERS OF WAR

CHAPTER I GENERAL OBSERVATIONS

ARTICLE 21

The Detaining Power may subject prisoners of war to internment. It may impose on them the obligation of not leaving, beyond certain limits, the camp where they are interned, or if the said camp is fenced in, of not going outside its perimeter. Subject to the provisions of the present Convention relative to penal and disciplinary sanctions, prisoners of war may not be held in close confinement except where necessary to safeguard their health and then only during the continuation of the circumstances which make such confinement necessary.

Prisoners of war may be partially or wholly released on parole or promise, in so far as is allowed by the laws of the Power on which they depend. Such measures shall be taken particularly in cases where this may contribute to the improvement of their state of health. No prisoner of war shall be compelled to accept liberty on parole or promise.

Upon the outbreak of hostilities, each Party to the conflict shall notify the adverse Party of the laws and regulations allowing or forbidding its own nationals to accept liberty on parole or promise. Prisoners of war who are paroled or who have given their promise in conformity with the laws and regulations so notified, are bound on their personal honor scrupulously to fulfil, both towards the Power on which they depend and towards the Power which has captured them, the engagements of their paroles or promises. In such cases, the Power on which they depend is bound neither to require nor to accept from them any service incompatible with the parole or promise given.

ARTICLE 22

Prisoners of war may be interned only in premises located on land and affording every guarantee of hygiene and healthfulness. Except in particular cases which are justified by the interest of the prisoners themselves, they shall not be interned in penitentiaries.

Prisoners of war interned in unhealthy areas, or where the climate is injurious for them, shall be removed as soon as possible to a more favorable climate.

The Detaining Power shall assemble prisoners of war in camps or camp compounds according to their nationality, language and customs, provided that such prisoners shall not be separated from prisoners of war belonging to the armed forces with which they were serving at the time of their capture, except with their consent.

ARTICLE 23

No prisoner of war may at any time be sent to or detained in areas where he may be exposed to the fire of the combat zone, nor may his presence be used to render certain points or areas immune from military operations.

Prisoners of war shall have shelters against air bombardment and other hazards of war, to the same extent as the local civilian population. With the exception of those engaged in the protection of their quarters against the aforesaid hazards, they may enter such shelters as soon as possible after the giving of the alarm. Any other protective measure taken in favor of the population shall also apply to them.

Detaining Powers shall give the Powers concerned, through the intermediary of the Protecting Powers, all useful information regarding the geographical location of prisoner of war camps.

Whenever military considerations permit, prisoner of war camps shall be indicated in the daytime by the letters PW or PG, placed so as to be clearly visible from the air. The Powers concerned may, however, agree upon any other system of marking. Only prisoner of war camps shall be marked as such.

ARTICLE 24

Transit or screening camps of a permanent kind shall be fitted out under conditions similar to those described in the present Section, and the prisoners therein shall have the same treatment as in other camps.

CHAPTER II QUARTERS, FOOD AND CLOTHING OF PRISONERS OF WAR

ARTICLE 25

Prisoners of war shall be quartered under conditions as favorable as those for the forces of the Detaining Power who are billeted in the same area. The said conditions shall make allowance for the habits and customs of the prisoners and shall in no case be prejudicial to their health.

The foregoing provisions shall apply in particular to the dormitories of prisoners of war as regards both total surface and minimum cubic space, and the general installations, bedding and blankets.

The premises provided for the use of prisoners of war individually or collectively, shall be entirely protected from dampness and adequately heated and lighted, in particular between dusk and lights out. All precautions must be taken against the danger of fire.

In any camps in which women prisoners of war, as well as men, are accommodated, separate dormitories shall be provided for them.

ARTICLE 26

The basic daily food rations shall be sufficient in quantity, quality and variety to keep prisoners of war in good health and to prevent loss of weight or the development of nutritional deficiencies. Account shall also be taken of the habitual diet of the prisoners.

The Detaining Power shall supply prisoners of war who work with such additional rations as are necessary for the labor on which they are employed.

Sufficient drinking water shall be supplied to prisoners of war. The use of tobacco shall be permitted.

Prisoners of war shall, as far as possible, be associated with the preparation of their meals; they may be employed for that purpose in the kitchens. Furthermore, they shall be given the means of preparing, themselves, the additional food in their possession.

Adequate premises shall be provided for messing.

Collective disciplinary measures affecting food are prohibited.

ARTICLE 27

Clothing, underwear and footwear shall be supplied to prisoners of war in sufficient quantities by the Detaining Power, which shall make allowance for the climate of the region where the prisoners are detained. Uniforms of enemy armed forces captured by the Detaining Power should, if suitable for the climate, be made available to clothe prisoners of war.

The regular replacement and repair of the above articles shall be assured by the Detaining Power. In addition, prisoners of war who work shall receive appropriate clothing, wherever the nature of the work demands.

ARTICLE 28

Canteens shall be installed in all camps, where prisoners of war may procure foodstuffs, soap and tobacco and ordinary articles in daily use. The tariff shall never be in excess of local market prices. The profits made by camp canteens shall be used for the benefit of the prisoners; a special fund shall be created for this purpose. The prisoners' representative shall have the right to collaborate in the management of the canteen and of this fund.

When a camp is closed down, the credit balance of the special fund shall be handed to an international welfare organization, to be employed for the benefit of prisoners of war of the same

nationality as those who have contributed to the fund. In case of a general repatriation, such profits shall be kept by the Detaining Power, subject to any agreement to the contrary between the Powers concerned

CHAPTER III HYGIENE AND MEDICAL ATTENTION

ARTICLE 29

The Detaining Power shall be bound to take all sanitary measures necessary to ensure the cleanliness and healthfulness of camps and to prevent epidemics.

Prisoners of war shall have for their use, day and night, conveniences which conform to the rules of hygiene and are maintained in a constant state of cleanliness. In any camps in which women prisoners of war are accommodated, separate conveniences shall be provided for them.

Also, apart from the baths and showers with which the camps shall be furnished, prisoners of war shall be provided with sufficient water and soap for their personal toilet and for washing their personal laundry; the necessary installations, facilities and time shall be granted them for that purpose.

ARTICLE 30

Every camp shall have an adequate infirmary where prisoners of war may have the attention they require, as well as appropriate diet. Isolation wards shall, if necessary, be set aside for cases of contagious or mental disease.

Prisoners of war suffering from serious disease, or whose condition necessitates special treatment, a surgical operation or hospital care, must be admitted to any military or civilian medical unit where such treatment can be given, even if their repatriation is contemplated in the near future. Special facilities shall be afforded for the care to be given to the disabled, in particular to the blind, and for their rehabilitation, pending repatriation.

Prisoners of war shall have the attention, preferably, of medical personnel of the Power on which they depend and, if possible, of their nationality.

Prisoners of war may not be prevented from presenting themselves to the medical authorities for examination. The detaining authorities shall, upon request, issue to every prisoner who has undergone treatment, an official certificate indicating the nature of his illness or injury, and the duration and kind of treatment received. A duplicate of this certificate shall be forwarded to the Central Prisoners of War Agency.

The costs of treatment, including those of any apparatus necessary for the maintenance of prisoners of war in good health, particularly dentures and other artificial appliances, and spectacles, shall be borne by the Detaining Power.

ARTICLE 31

Medical inspections of prisoners of war shall be held at least once a month. They shall include the checking and the recording of the weight of each prisoner of war. Their purpose shall be, in particular, to supervise the general state of health, nutrition and cleanliness of prisoners and to detect contagious diseases, especially tuberculosis, malaria and venereal disease. For this

purpose the most efficient methods available shall be employed, e.g. periodic mass miniature radiography for the early detection of tuberculosis.

ARTICLE 32

Prisoners of war who, though not attached to the medical service of their armed forces, are physicians, surgeons, dentists, nurses or medical orderlies, may be required by the Detaining Power to exercise their medical functions in the interests of prisoners of war dependent on the same Power. In that case they shall continue to be prisoners of war, but shall receive the same treatment as corresponding medical personnel retained by the Detaining Power. They shall be exempted from any other work under Article 49.

Chapter IV Medical Personnel and Chaplains Retained To Assist Prisoners Of War

ARTICLE 33

Members of the medical personnel and chaplains while retained by the Detaining Power with a view to assisting prisoners of war, shall not be considered as prisoners of war. They shall, however, receive as a minimum the benefits and protection of the present Convention, and shall also be granted all facilities necessary to provide for the medical care of, and religious ministration to, prisoners of war.

They shall continue to exercise their medical and spiritual functions for the benefit of prisoners of war, preferably those belonging to the armed forces upon which they depend, within the scope of the military laws and regulations of the Detaining Power and under the control of its competent services, in accordance with their professional etiquette. They shall also benefit by the following facilities in the exercise of their medical or spiritual functions:

(a) They shall be authorized to visit periodically prisoners of war situated in working detachments or in hospitals outside the camp. For this purpose, the Detaining Power shall place at their disposal the necessary means of transport.

(b) The senior medical officer in each camp shall be responsible to the camp military authorities for everything connected with the activities of retained medical personnel. For this purpose, Parties to the conflict shall agree at the outbreak of hostilities on the subject of the corresponding ranks of the medical personnel, including that of societies mentioned in Article 26 of the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of August 12, 1949. This senior medical officer, as well as chaplains, shall have the right to deal with the competent authorities of the camp on all questions relating to their duties. Such authorities shall afford them all necessary facilities for correspondence relating to these questions.

(c) Although they shall be subject to the internal discipline of the camp in which they are retained, such personnel may not be compelled to carry out any work other than that concerned with their medical or religious duties.

During hostilities, the Parties to the conflict shall agree concerning the possible relief of retained personnel and shall settle the procedure to be followed.

None of the preceding provisions shall relieve the Detaining Power of its obligations with regard to prisoners of war from the medical or spiritual point of view.

CHAPTER V RELIGIOUS, INTELLECTUAL AND PHYSICAL ACTIVITIES

ARTICLE 34

Prisoners of war shall enjoy complete latitude in the exercise of their religious duties, including attendance at the service of their faith, on condition that they comply with the disciplinary routine prescribed by the military authorities.

Adequate premises shall be provided where religious services may be held.

ARTICLE 35

Chaplains who fall into the hands of the enemy Power and who remain or are retained with a view to assisting prisoners of war, shall be allowed to minister to them and to exercise freely their ministry amongst prisoners of war of the same religion, in accordance with their religious conscience. They shall be allocated among the various camps and labor detachments containing prisoners of war belonging to the same forces, speaking the same language or practicing the same religion. They shall enjoy the necessary facilities, including the means of transport provided for in Article 33, for visiting the prisoners of war outside their camp. They shall be free to correspond, subject to censorship, on matters concerning their religious duties with the ecclesiastical authorities in the country of detention and with international religious organizations. Letters and cards which they may send for this purpose shall be in addition to the quota provided for in Article 71.

ARTICLE 36

Prisoners of war who are ministers of religion, without having officiated as chaplains to their own forces, shall be at liberty, whatever their denomination, to minister freely to the members of their community. For this purpose, they shall receive the same treatment as the chaplains retained by the Detaining Power. They shall not be obliged to do any other work.

ARTICLE 37

When prisoners of war have not the assistance of a retained chaplain or of a prisoner of war minister of their faith, a minister belonging to the prisoners' or a similar denomination, or in his absence a qualified layman, if such a course is feasible from a confessional point of view, shall be appointed, at the request of the prisoners concerned, to fill this office. This appointment, subject to the approval of the Detaining Power, shall take place with the agreement of the community of prisoners concerned and, wherever necessary, with the approval of the local religious authorities of the same faith. The person thus appointed shall comply with all regulations established by the Detaining Power in the interests of discipline and military security.

ARTICLE 38

While respecting the individual preferences of every prisoner, the Detaining Power shall encourage the practice of intellectual, educational, and recreational pursuits, sports and games amongst prisoners, and shall take the measures necessary to ensure the exercise thereof by providing them with adequate premises and necessary equipment.

Prisoners shall have opportunities for taking physical exercise, including sports and games, and for being out of doors. Sufficient open spaces shall be provided for this purpose in all camps.

CHAPTER VI DISCIPLINE

ARTICLE 39

Every prisoner of war camp shall be put under the immediate authority of a responsible commissioned officer belonging to the regular armed forces of the Detaining Power. Such officer shall have in his possession a copy of the present Convention; he shall ensure that its provisions are known to the camp staff and the guard and shall be responsible, under the direction of his government, for its application.

Prisoners of war, with the exception of officers, must salute and show to all officers of the Detaining Power the external marks of respect provided for by the regulations applying in their own forces.

Officer prisoners of war are bound to salute only officers of a higher rank of the Detaining Power; they must, however, salute the camp commander regardless of his rank.

ARTICLE 40

The wearing of badges of rank and nationality, as well as of decorations, shall be permitted.

ARTICLE 41

In every camp the text of the present Convention and its Annexes and the contents of any special agreement provided for in Article 6, shall be posted, in the prisoners' own language, at places where all may read them. Copies shall be supplied, on request, to the prisoners who cannot have access to the copy which has been posted.

Regulations, orders, notices and publications of every kind relating to the conduct of prisoners of war shall be issued to them in a language which they understand. Such regulations, orders and publications shall be posted in the manner described above and copies shall be handed to the prisoners' representative. Every order and command addressed to prisoners of war individually must likewise be given in a language which they understand.

ARTICLE 42

The use of weapons against prisoners of war, especially against those who are escaping or attempting to escape, shall constitute an extreme measure, which shall always be preceded by warnings appropriate to the circumstances.

CHAPTER VII RANK OF PRISONERS OF WAR

ARTICLE 43

Upon the outbreak of hostilities, the Parties to the conflict shall communicate to one another the titles and ranks of all the persons mentioned in Article 4 of the present Convention, in order to ensure equality of treatment between prisoners of equivalent rank. Titles and ranks which are subsequently created shall form the subject of similar communications.

The Detaining Power shall recognize promotions in rank which have been accorded to prisoners of war and which have been duly notified by the Power on which these prisoners depend.

ARTICLE 44

Officers and prisoners of equivalent status shall be treated with the regard due to their rank and age.

In order to ensure service in officers' camps, other ranks of the same armed forces who, as far as possible, speak the same language, shall be assigned in sufficient numbers, account being taken of the rank of officers and prisoners of equivalent status. Such orderlies shall not be required to perform any other work.

Supervision of the mess by the officers themselves shall be facilitated in every way.

ARTICLE 45

Prisoners of war other than officers and prisoners of equivalent status shall be treated with the regard due to their rank and age.

Supervision of the mess by the prisoners themselves shall be facilitated in every way.

CHAPTER VIII TRANSFER OF PRISONERS OF WAR AFTER THEIR ARRIVAL IN CAMP

ARTICLE 46

The Detaining Power, when deciding upon the transfer of prisoners of war, shall take into account the interests of the prisoners themselves, more especially so as not to increase the difficulty of their repatriation.

The transfer of prisoners of war shall always be effected humanely and in conditions not less favorable than those under which the forces of the Detaining Power are transferred. Account shall always be taken of the climatic conditions to which the prisoners of war are accustomed and the conditions of transfer shall in no case be prejudicial to their health.

The Detaining Power shall supply prisoners of war during transfer with sufficient food and drinking water to keep them in good health, likewise with the necessary clothing, shelter and medical attention. The Detaining Power shall take adequate precautions especially in case of transport by sea or by air, to ensure their safety during transfer, and shall draw up a complete list of all transferred prisoners before their departure.

ARTICLE 47

Sick or wounded prisoners of war shall not be transferred as long as their recovery may be endangered by the journey, unless their safety imperatively demands it.

If the combat zone draws closer to a camp, the prisoners of war in the said camp shall not be transferred unless their transfer can be carried out in adequate conditions of safety, or if they are exposed to greater risks by remaining on the spot than by being transferred.

ARTICLE 48

In the event of transfer, prisoners of war shall be officially advised of their departure and of their new postal address. Such notifications shall be given in time for them to pack their luggage and inform their next of kin.

They shall be allowed to take with them their personal effects, and the correspondence and parcels which have arrived for them. The weight of such baggage may be limited, if the conditions of transfer so require, to what each prisoner can reasonably carry, which shall in no case be more than twenty-five kilograms per head.

Mail and parcels addressed to their former camp shall be forwarded to them without delay. The camp commander shall take, in agreement with the prisoners' representative, any measures needed to ensure the transport of the prisoners' community property and of the luggage they are unable to take with them in consequence of restrictions imposed by virtue of the second paragraph of this Article.

The costs of transfers shall be borne by the Detaining Power.

SECTION III LABOR OF PRISONERS OF WAR

ARTICLE 49

The Detaining Power may utilize the labor of prisoners of war who are physically fit, taking into account their age, sex, rank and physical aptitude, and with a view particularly to maintaining them in a good state of physical and mental health.

Non-commissioned officers who are prisoners of war shall only be required to do supervisory work. Those not so required may ask for other suitable work which shall, so far as possible, be found for them.

If officers or persons of equivalent status ask for suitable work, it shall be found for them, so far as possible, but they may in no circumstances be compelled to work.

ARTICLE 50

Besides work connected with camp administration, installation or maintenance, prisoners of war may be compelled to do only such work as is included in the following classes:

(a) Agriculture;

(b) Industries connected with the production or the extraction of raw materials, and manufacturing industries, with the exception of metallurgical, machinery and chemical industries; public works and building operations which have no military character or purpose;

(c) Transport and handling of stores which are not military in character or purpose;

(d) Commercial business, and arts and crafts;

(e) Domestic service;

(f) Public utility services having no military character or purpose.

Should the above provisions be infringed, prisoners of war shall be allowed to exercise their right of complaint, in conformity with Article 78.

ARTICLE 51

Prisoners of war must be granted suitable working conditions, especially as regards accommodation, food, clothing and equipment; such conditions shall not be inferior to those enjoyed by nationals of the Detaining Power employed in similar work; account shall also be taken of climatic conditions.

The Detaining Power, in utilizing the labor of prisoners of war, shall ensure that in areas in which prisoners are employed, the national legislation concerning the protection of labor, and, more particularly, the regulations for the safety of workers, are duly applied.

Prisoners of war shall receive training and be provided with the means of protection suitable to the work they will have to do and similar to those accorded to the nationals of the Detaining Power. Subject to the provisions of Article 52, prisoners may be submitted to the normal risks run by these civilian workers.

Conditions of labor shall in no case be rendered more arduous by disciplinary measures.

ARTICLE 52

Unless he be a volunteer, no prisoner of war may be employed on labor which is of an unhealthy or dangerous nature.

No prisoner of war shall be assigned to labor which would be looked upon as humiliating for a member of the Detaining Power's own forces.

The removal of mines or similar devices shall be considered as dangerous labor.

ARTICLE 53

The duration of the daily labor of prisoners of war, including the time of the journey to and fro, shall not be excessive, and must in no case exceed that permitted for civilian workers in the district, who are nationals of the Detaining Power and employed on the same work.

Prisoners of war must be allowed, in the middle of the day's work, a rest of not less than one hour. This rest will be the same as that to which workers of the Detaining Power are entitled, if the latter is of longer duration. They shall be allowed in addition a rest of twenty-four consecutive hours every week, preferably on Sunday or the day of rest in their country of origin. Furthermore, every prisoner who has worked for one year shall be granted a rest of eight consecutive days, during which his working pay shall be paid him.

If methods of labor such as piecework are employed, the length of the working period shall not be rendered excessive thereby.

ARTICLE 54

The working pay due to prisoners of war shall be fixed in accordance with the provisions of Article 62 of the present Convention.

Prisoners of war who sustain accidents in connection with work, or who contract a disease in the course, or in consequence of their work, shall receive all the care their condition may require. The Detaining Power shall furthermore deliver to such prisoners of war a medical certificate enabling them to submit their claims to the Power on which they depend, and shall send a duplicate to the Central Prisoners of War Agency provided for in Article 123.

ARTICLE 55

The fitness of prisoners of war for work shall be periodically verified by medical examinations at least once a month. The examinations shall have particular regard to the nature of the work which prisoners of war are required to do.

If any prisoner of war considers himself incapable of working, he shall be permitted to appear before the medical authorities of his camp. Physicians or surgeons may recommend that the prisoners who are, in their opinion, unfit for work, be exempted therefrom.

ARTICLE 56

The organization and administration of labor detachments shall be similar to those of prisoner of war camps.

Every labor detachment shall remain under the control of and administratively part of a prisoner of war camp. The military authorities and the commander of the said camp shall be responsible, under the direction of their government, for the observance of the provisions of the present Convention in labor detachments.

The camp commander shall keep an up-to-date record of the labor detachments dependent on his camp, and shall communicate it to the delegates of the Protecting Power, of the International Committee of the Red Cross, or of other agencies giving relief to prisoners of war, who may visit the camp.

ARTICLE 57

The treatment of prisoners of war who work for private persons, even if the latter are responsible for guarding and protecting them, shall not be inferior to that which is provided for by the present Convention. The Detaining Power, the military authorities and the commander of the camp to which such prisoners belong shall be entirely responsible for the maintenance, care, treatment, and payment of the working pay of such prisoners of war.

Such prisoners of war shall have the right to remain in communication with the prisoners' representatives in the camps on which they depend.

SECTION IV FINANCIAL RESOURCES OF PRISONERS OF WAR

ARTICLE 58

Upon the outbreak of hostilities, and pending an arrangement on this matter with the Protecting Power, the Detaining Power may determine the maximum amount of money in cash or in any similar form that prisoners may have in their possession. Any amount in excess, which was properly in their possession and which has been taken or withheld from them, shall be placed to their account, together with any monies deposited by them, and shall not be converted into any other currency without their consent.

If prisoners of war are permitted to purchase services or commodities outside the camp against payment in cash, such payments shall be made by the prisoner himself or by the camp administration who will charge them to the accounts of the prisoners concerned. The Detaining Power will establish the necessary rules in this respect.

ARTICLE 59

Cash which was taken from prisoners of war, in accordance with Article 18, at the time of their capture, and which is in the currency of the Detaining Power, shall be placed to their separate accounts, in accordance with the provisions of Article 64 of the present Section.

The amounts, in the currency of the Detaining Power, due to the conversion of sums in other currencies that are taken from the prisoners of war at the same time, shall also be credited to their separate accounts.

ARTICLE 60

The Detaining Power shall grant all prisoners of war a monthly advance of pay, the amount of which shall be fixed by conversion, into the currency of the said Power, of the following amounts:

Category I: Prisoners ranking below sergeant: eight Swiss francs.

Category II: Sergeants and other non-commissioned officers, or prisoners of equivalent rank: twelve Swiss francs.

Category III: Warrant officers and commissioned officers below the rank of major or prisoners of equivalent rank: fifty Swiss francs.

Category IV: Majors, lieutenant colonels, colonels or prisoners of equivalent rank: sixty Swiss francs.

Category V: General officers or prisoners of equivalent rank: seventy-five Swiss francs.

However, the Parties to the conflict concerned may by special agreement modify the amount of advances of pay due to prisoners of the preceding categories.

Furthermore, if the amounts indicated in the first paragraph above would be unduly high compared with the pay of the Detaining Power's armed forces or would, for any reason, seriously embarrass the Detaining Power, then, pending the conclusion of a special agreement with the Power on which the prisoners depend to vary the amounts indicated above, the Detaining Power:

(a) Shall continue to credit the accounts of the prisoners with the amounts indicated in the first paragraph above;

(b) May temporarily limit the amount made available from these advances of pay to prisoners of war for their own use, to sums which are reasonable, but which, for Category I, shall never be inferior to the amount that the Detaining Power gives to the members of its own armed forces.

The reasons for any limitations will be given without delay to the Protecting Power.

ARTICLE 61

The Detaining Power shall accept for distribution as supplementary pay to prisoners of war sums which the Power on which the prisoners depend may forward to them, on condition that the sums to be paid shall be the same for each prisoner of the same category, shall be payable to all prisoners of that category depending on that Power, and shall be placed in their separate accounts, at the earliest opportunity, in accordance with the provisions of Article 64. Such supplementary pay shall not relieve the Detaining Power of any obligation under this Convention.

ARTICLE 62

Prisoners of war shall be paid a fair working rate of pay by the detaining authorities direct. The rate shall be fixed by the said authorities, but shall at no time be less than one-fourth of one Swiss franc for a full working day. The Detaining Power shall inform prisoners of war, as well as the Power on which they depend, through the intermediary of the Protecting Power, of the rate of daily working pay that it has fixed.

Working pay shall likewise be paid by the detaining authorities to prisoners of war permanently detailed to duties or to a skilled or semi-skilled occupation in connection with the administration, installation or maintenance of camps, and to the prisoners who are required to carry out spiritual or medical duties on behalf of their comrades.

The working pay of the prisoners' representative, of his advisers, if any, and of his assistants, shall be paid out of the fund maintained by canteen profits. The scale of this working pay shall be fixed by the prisoners' representative and approved by the camp commander. If there is no such fund, the detaining authorities shall pay these prisoners a fair working rate of pay.

ARTICLE 63

Prisoners of war shall be permitted to receive remittances of money addressed to them individually or collectively.

Every prisoner of war shall have at his disposal the credit balance of his account as provided for in the following Article, within the limits fixed by the Detaining Power, which shall make such payments as are requested. Subject to financial or monetary restrictions which the Detaining Power regards as essential, prisoners of war may also have payments made abroad. In this case payments addressed by prisoners of war to dependants shall be given priority.

In any event, and subject to the consent of the Power on which they depend, prisoners may have payments made in their own country, as follows: the Detaining Power shall send to the aforesaid

Power through the Protecting Power a notification giving all the necessary particulars concerning the prisoners of war, the beneficiaries of the payments, and the amount of the sums to be paid, expressed in the Detaining Power's currency. The said notification shall be signed by the prisoners and countersigned by the camp commander. The Detaining Power shall debit the prisoners' account by a corresponding amount; the sums thus debited shall be placed by it to the credit of the Power on which the prisoners depend.

To apply the foregoing provisions, the Detaining Power may usefully consult the Model Regulations in Annex V of the present Convention.

ARTICLE 64

The Detaining Power shall hold an account for each prisoner of war, showing at least the following:

1. The amounts due to the prisoner or received by him as advances of pay, as working pay or derived from any other source; the sums in the currency of the Detaining Power which were taken from him; the sums taken from him and converted at his request into the currency of the said Power.

2. The payments made to the prisoner in cash, or in any other similar form; the payments made on his behalf and at his request; the sums transferred under Article 63, third paragraph.

ARTICLE 65

Every item entered in the account of a prisoner of war shall be countersigned or initialed by him, or by the prisoners' representative acting on his behalf.

Prisoners of war shall at all times be afforded reasonable facilities for consulting and obtaining copies of their accounts, which may likewise be inspected by the representatives of the Protecting Powers at the time of visits to the camp.

When prisoners of war are transferred from one camp to another, their personal accounts will follow them. In case of transfer from one Detaining Power to another, the monies which are their property and are not in the currency of the Detaining Power will follow them. They shall be given certificates for any other monies standing to the credit of their accounts.

The Parties to the conflict concerned may agree to notify to each other at specific intervals through the Protecting Power, the amount of the accounts of the prisoners of war.

ARTICLE 66

On the termination of captivity, through the release of a prisoner of war or his repatriation, the Detaining Power shall give him a statement, signed by an authorized officer of that Power, showing the credit balance then due to him. The Detaining Power shall also send through the Protecting Power to the government upon which the prisoner of war depends, lists giving all appropriate particulars of all prisoners of war whose captivity has been terminated by repatriation, release, escape, death or any other means, and showing the amount of their credit balances. Such lists shall be certified on each sheet by an authorized representative of the Detaining Power.

Any of the above provisions of this Article may be varied by mutual agreement between any two Parties to the conflict.

The Power on which the prisoner of war depends shall be responsible for settling with him any credit balance due to him from the Detaining Power on the termination of his captivity.

ARTICLE 67

Advances of pay, issued to prisoners of war in conformity with Article 60, shall be considered as made on behalf of the Power on which they depend. Such advances of pay, as well as all payments made by the said Power under Article 63, third paragraph, and Article 68, shall form the subject of arrangements between the Powers concerned, at the close of hostilities.

ARTICLE 68

Any claim by a prisoner of war for compensation in respect of any injury or other disability arising out of work shall be referred to the Power on which he depends, through the Protecting Power. In accordance with Article 54, the Detaining Power will, in all cases, provide the prisoner of war concerned with a statement showing the nature of the injury or disability, the circumstances in which it arose and particulars of medical or hospital treatment given for it. This statement will be signed by a responsible officer of the Detaining Power and the medical particulars certified by a medical officer.

Any claim by a prisoner of war for compensation in respect of personal effects, monies or valuables impounded by the Detaining Power under Article 18 and not forthcoming on his repatriation, or in respect of loss alleged to be due to the fault of the Detaining Power or any of its servants, shall likewise be referred to the Power on which he depends. Nevertheless, any such personal effects required for use by the prisoners of war whilst in captivity shall be replaced at the expense of the Detaining Power. The Detaining Power will, in all cases, provide the prisoner of war with a statement, signed by a responsible officer, showing all available information regarding the reasons why such effects, monies or valuables have not been restored to him. A copy of this statement will be forwarded to the Power on which he depends through the Central Prisoners of War Agency provided for in Article 123.

SECTION V RELATIONS OF PRISONERS OF WAR WITH THE EXTERIOR

ARTICLE 69

Immediately upon prisoners of war falling into its power, the Detaining Power shall inform them and the Powers on which they depend, through the Protecting Power, of the measures taken to carry out the provisions of the present Section. They shall likewise inform the parties concerned of any subsequent modifications of such measures.

ARTICLE 70

Immediately upon capture, or not more than one week after arrival at a camp, even if it is a transit camp, likewise in case of sickness or transfer to hospital or another camp, every prisoner of war shall be enabled to write direct to his family, on the one hand, and to the Central

Prisoners of War Agency provided for in Article 123, on the other hand, a card similar, if possible, to the model annexed to the present Convention, informing his relatives of his capture, address and state of health. The said cards shall be forwarded as rapidly as possible and may not be delayed in any manner.

ARTICLE 71

Prisoners of war shall be allowed to send and receive letters and cards. If the Detaining Power deems it necessary to limit the number of letters and cards sent by each prisoner of war, the said number shall not be less than two letters and four cards monthly, exclusive of the capture cards provided for in Article 70, and conforming as closely as possible to the models annexed to the present Convention. Further limitations may be imposed only if the Protecting Power is satisfied that it would be in the interests of the prisoners of war concerned to do so owing to difficulties of translation caused by the Detaining Power's inability to find sufficient qualified linguists to carry out the necessary censorship. If limitations must be placed on the correspondence addressed to prisoners of war, they may be ordered only by the Power on which the prisoners depend, possibly at the request of the Detaining Power. Such letters and cards must be conveyed by the most rapid method at the disposal of the Detaining Power; they may not be delayed or retained for disciplinary reasons.

Prisoners of war who have been without news for a long period, or who are unable to receive news from their next of kin or to give them news by the ordinary postal route, as well as those who are at a great distance from their homes, shall be permitted to send telegrams, the fees being charged against the prisoners of war's accounts with the Detaining Power or paid in the currency at their disposal. They shall likewise benefit by this measure in cases of urgency.

As a general rule, the correspondence of prisoners of war shall be written in their native language. The Parties to the conflict may allow correspondence in other languages.

Sacks containing prisoner of war mail must be securely sealed and labeled so as clearly to indicate their contents, and must be addressed to offices of destination.

ARTICLE 72

Prisoners of war shall be allowed to receive by post or by any other means individual parcels or collective shipments containing, in particular, foodstuffs, clothing, medical supplies and articles of a religious, educational or recreational character which may meet their needs, including books, devotional articles, scientific equipment, examination papers, musical instruments, sports outfits and materials allowing prisoners of war to pursue their studies or their cultural activities.

Such shipments shall in no way free the Detaining Power from the obligations imposed upon it by virtue of the present Convention.

The only limits which may be placed on these shipments shall be those proposed by the Protecting Power in the interest of the prisoners themselves, or by the International Committee of the Red Cross or any other organization giving assistance to the prisoners, in respect of their own shipments only, on account of exceptional strain on transport or communications.

The conditions for the sending of individual parcels and collective relief shall, if necessary, be the subject of special agreements between the Powers concerned, which may in no case delay the

receipt by the prisoners of relief supplies. Books may not be included in parcels of clothing and foodstuffs. Medical supplies shall, as a rule, be sent in collective parcels.

ARTICLE 73

In the absence of special agreements between the Powers concerned on the conditions for the receipt and distribution of collective relief shipments, the rules and regulations concerning collective shipments, which are annexed to the present Convention, shall be applied.

The special agreements referred to above shall in no case restrict the right of prisoners' representatives to take possession of collective relief shipments intended for prisoners of war, to proceed to their distribution or to dispose of them in the interest of the prisoners.

Nor shall such agreements restrict the right of representatives of the Protecting Power, the International Committee of the Red Cross or any other organization giving assistance to prisoners of war and responsible for the forwarding of collective shipments, to supervise their distribution to the recipients.

ARTICLE 74

All relief shipments for prisoners of war shall be exempt from import, customs and other dues.

Correspondence, relief shipments and authorized remittances of money addressed to prisoners of war or dispatched by them through the post office, either direct or through the Information Bureau provided for in Article 122 and the Central Prisoners of War Agency provided for in Article 123, shall be exempt from any postal dues, both in the countries of origin and destination, and in intermediate countries.

If relief shipments intended for prisoners of war cannot be sent through the post office by reason of weight or for any other cause, the cost of transportation shall be borne by the Detaining Power in all the territories under its control. The other Powers party to the Convention shall bear the cost of transport in their respective territories.

In the absence of special agreements between the Parties concerned, the costs connected with transport of such shipments, other than costs covered by the above exemption, shall be charged to the senders.

The High Contracting Parties shall endeavor to reduce, so far as possible, the rates charged for telegrams sent by prisoners of war, or addressed to them.

ARTICLE 75

Should military operations prevent the Powers concerned from fulfilling their obligation to assure the transport of the shipments referred to in Articles 70, 71, 72 and 77, the Protecting Powers concerned, the International Committee of the Red Cross or any other organization duly approved by the Parties to the conflict may undertake to ensure the conveyance of such shipments by suitable means (railway wagons, motor vehicles, vessels or aircraft, etc.). For this purpose, the High Contracting Parties shall endeavor to supply them with such transport and to allow its circulation, especially by granting the necessary safe-conducts.

Such transport may also be used to convey:

(a) Correspondence, lists and reports exchanged between the Central Information Agency referred to in Article 123 and the National Bureau referred to in Article 122;

(b) Correspondence and reports relating to prisoners of war which the Protecting Powers, the International Committee of the Red Cross or any other body assisting the prisoners, exchange either with their own delegates or with the Parties to the conflict.

These provisions in no way detract from the right of any Party to the conflict to arrange other means of transport, if it should so prefer, nor preclude the granting of safe-conducts, under mutually agreed conditions, to such means of transport.

In the absence of special agreements, the costs occasioned by the use of such means of transport shall be borne proportionally by the Parties to the conflict whose nationals are benefited thereby.

ARTICLE 76

The censoring of correspondence addressed to prisoners of war or dispatched by them shall be done as quickly as possible. Mail shall be censored only by the dispatching State and the receiving State, and once only by each.

The examination of consignments intended for prisoners of war shall not be carried out under conditions that will expose the goods contained in them to deterioration; except in the case of written or printed matter, it shall be done in the presence of the addressee, or of a fellow-prisoner duly delegated by him. The delivery to prisoners of individual or collective consignments shall not be delayed under the pretext of difficulties of censorship.

Any prohibition of correspondence ordered by Parties to the conflict, either for military or political reasons, shall be only temporary and its duration shall be as short as possible.

ARTICLE 77

The Detaining Powers shall provide all facilities for the transmission, through the Protecting Power or the Central Prisoners of War Agency provided for in Article 123, of instruments, papers or documents intended for prisoners of war or dispatched by them, especially powers of attorney and wills.

In all cases they shall facilitate the preparation and execution of such documents on behalf of prisoners of war; in particular, they shall allow them to consult a lawyer and shall take what measures are necessary for the authentication of their signatures.

SECTION VI RELATIONS BETWEEN PRISONERS OF WAR AND THE AUTHORITIES

CHAPTER I COMPLAINTS OF PRISONERS OF WAR RESPECTING THE CONDITIONS OF CAPTIVITY

ARTICLE 78

Prisoners of war shall have the right to make known to the military authorities in whose power they are, their requests regarding the conditions of captivity to which they are subjected.

They shall also have the unrestricted right to apply to the representatives of the Protecting Powers either through their prisoners' representative or, if they consider it necessary, direct, in order to draw their attention to any points on which they may have complaints to make regarding their conditions of captivity.

These requests and complaints shall not be limited nor considered to be a part of the correspondence quota referred to in Article 71. They must be transmitted immediately. Even if they are recognized to be unfounded, they may not give rise to any punishment.

Prisoners' representatives may send periodic reports on the situation in the camps and the needs of the prisoners of war to the representatives of the Protecting Powers.

CHAPTER II PRISONER OF WAR REPRESENTATIVES

ARTICLE 79

In all places where there are prisoners of war, except in those where there are officers, the prisoners shall freely elect by secret ballot, every six months, and also in case of vacancies, prisoners' representatives entrusted with representing them before the military authorities, the Protecting Powers, the International Committee of the Red Cross and any other organization which may assist them. These prisoners' representatives shall be eligible for re-election.

In camps for officers and persons of equivalent status or in mixed camps, the senior officer among the prisoners of war shall be recognized as the camp prisoners' representative. In camps for officers, he shall be assisted by one or more advisers chosen by the officers; in mixed camps, his assistants shall be chosen from among the prisoners of war who are not officers and shall be elected by them.

Officer prisoners of war of the same nationality shall be stationed in labor camps for prisoners of war, for the purpose of carrying out the camp administration duties for which the prisoners of war are responsible. These officers may be elected as prisoners' representatives under the first paragraph of this Article. In such a case the assistants to the prisoners' representatives shall be chosen from among those prisoners of war who are not officers.

Every representative elected must be approved by the Detaining Power before he has the right to commence his duties. Where the Detaining Power refuses to approve a prisoner of war elected by his fellow prisoners of war, it must inform the Protecting Power of the reason for such refusal.

In all cases the prisoners' representative must have the same nationality, language and customs as the prisoners of war whom he represents. Thus, prisoners of war distributed in different sections of a camp, according to their nationality, language or customs, shall have for each section their own prisoners' representative, in accordance with the foregoing paragraphs.

ARTICLE 80

Prisoners' representatives shall further the physical, spiritual and intellectual well being of prisoners of war.

In particular, where the prisoners decide to organize amongst themselves a system of mutual assistance, this organization will be within the province of the prisoners' representative, in addition to the special duties entrusted to him by other provisions of the present Convention.

Prisoners' representatives shall not be held responsible, simply by reason of their duties, for any offences committed by prisoners of war.

ARTICLE 81

Prisoners' representatives shall not be required to perform any other work, if the accomplishment of their duties is thereby made more difficult.

Prisoners' representatives may appoint from amongst the prisoners such assistants as they may require. All material facilities shall be granted them, particularly a certain freedom of movement necessary for the accomplishment of their duties (inspection of labor detachments, receipt of supplies, etc.).

Prisoners' representatives shall be permitted to visit premises where prisoners of war are detained, and every prisoner of war shall have the right to consult freely his prisoners' representative.

All facilities shall likewise be accorded to the prisoners' representatives for communication by post and telegraph with the detaining authorities, the Protecting Powers, the International Committee of the Red Cross and their delegates, the Mixed Medical Commissions and with the bodies which give assistance to prisoners of war. Prisoners' representatives of labor detachments shall enjoy the same facilities for communication with the prisoners' representatives of the principal camp. Such communications shall not be restricted, nor considered as forming a part of the quota mentioned in Article 71.

Prisoners' representatives who are transferred shall be allowed a reasonable time to acquaint their successors with current affairs.

In case of dismissal, the reasons therefor shall be communicated to the Protecting Power.

CHAPTER III PENAL AND DISCIPLINARY SANCTIONS

I. GENERAL PROVISIONS

ARTICLE 82

A prisoner of war shall be subject to the laws, regulations and orders in force in the armed forces of the Detaining Power; the Detaining Power shall be justified in taking judicial or disciplinary measures in respect of any offence committed by a prisoner of war against such laws, regulations or orders. However, no proceedings or punishments contrary to the provisions of this Chapter shall be allowed.

If any law, regulation or order of the Detaining Power shall declare acts committed by a prisoner of war to be punishable, whereas the same acts would not be punishable if committed by a member of the forces of the Detaining Power, such acts shall entail disciplinary punishments only.

ARTICLE 83

In deciding whether proceedings in respect of an offence alleged to have been committed by a prisoner of war shall be judicial or disciplinary, the Detaining Power shall ensure that the competent authorities exercise the greatest leniency and adopt, wherever possible, disciplinary rather than judicial measures.

ARTICLE 84

A prisoner of war shall be tried only by a military court, unless the existing laws of the Detaining Power expressly permit the civil courts to try a member of the armed forces of the Detaining Power in respect of the particular offence alleged to have been committed by the prisoner of war.

In no circumstances whatever shall a prisoner of war be tried by a court of any kind which does not offer the essential guarantees of independence and impartiality as generally recognized, and, in particular, the procedure of which does not afford the accused the rights and means of defense provided for in Article 105.

ARTICLE 85

Prisoners of war prosecuted under the laws of the Detaining Power for acts committed prior to capture shall retain, even if convicted, the benefits of the present Convention.

ARTICLE 86

No prisoner of war may be punished more than once for the same act, or on the same charge.

ARTICLE 87

Prisoners of war may not be sentenced by the military authorities and courts of the Detaining Power to any penalties except those provided for in respect of members of the armed forces of the said Power who have committed the same acts.

When fixing the penalty, the courts or authorities of the Detaining Power shall take into consideration, to the widest extent possible, the fact that the accused, not being a national of the Detaining Power, is not bound to it by any duty of allegiance, and that he is in its power as the result of circumstances independent of his own will. The said courts or authorities shall be at liberty to reduce the penalty provided for the violation of which the prisoner of war is accused, and shall therefore not be bound to apply the minimum penalty prescribed.

Collective punishment for individual acts, corporal punishments, imprisonment in premises without daylight and, in general, any form of torture or cruelty, are forbidden.

No prisoner of war may be deprived of his rank by the Detaining Power, or prevented from wearing his badges.

ARTICLE 88

Officers, non-commissioned officers and men who are prisoners of war undergoing a disciplinary or judicial punishment, shall not be subjected to more severe treatment than that applied in respect of the same punishment to members of the armed forces of the Detaining Power of equivalent rank.

A woman prisoner of war shall not be awarded or sentenced to a punishment more severe, or treated whilst undergoing punishment more severely, than a woman member of the armed forces of the Detaining Power dealt with for a similar offence.

In no case may a woman prisoner of war be awarded or sentenced to a punishment more severe, or treated whilst undergoing punishment more severely, than a male member of the armed forces of the Detaining Power dealt with for a similar offence.

Prisoners of war who have served disciplinary or judicial sentences may not be treated differently from other prisoners of war.

II. DISCIPLINARY SANCTIONS

ARTICLE 89

The disciplinary punishments applicable to prisoners of war are the following:

1. A fine which shall not exceed 50 per cent of the advances of pay and working pay which the prisoner of war would otherwise receive under the provisions of Articles 60 and 62 during a period of not more than thirty days.

2. Discontinuance of privileges granted over and above the treatment provided for by the present Convention.

3. Fatigue duties not exceeding two hours daily.

4. Confinement.

The punishment referred to under (3) shall not be applied to officers.

In no case shall disciplinary punishments be inhuman, brutal or dangerous to the health of prisoners of war.

ARTICLE 90

The duration of any single punishment shall in no case exceed thirty days. Any period of confinement awaiting the hearing of a disciplinary offence or the award of disciplinary punishment shall be deducted from an award pronounced against a prisoner of war.

The maximum of thirty days provided above may not be exceeded, even if the prisoner of war is answerable for several acts at the same time when he is awarded punishment, whether such acts are related or not.

The period between the pronouncing of an award of disciplinary punishment and its execution shall not exceed one month.

When a prisoner of war is awarded a further disciplinary punishment, a period of at least three days shall elapse between the execution of any two of the punishments, if the duration of one of these is ten days or more.

ARTICLE 91

The escape of a prisoner of war shall be deemed to have succeeded when:

1. He has joined the armed forces of the Power on which he depends, or those of an allied Power;

2. He has left the territory under the control of the Detaining Power, or of an ally of the said Power;

3. He has joined a ship flying the flag of the Power on which he depends, or of an allied Power, in the territorial waters of the Detaining Power, the said ship not being under the control of the last-named Power.

Prisoners of war who have made good their escape in the sense of this Article and who are recaptured, shall not be liable to any punishment in respect of their previous escape.

ARTICLE 92

A prisoner of war who attempts to escape and is recaptured before having made good his escape in the sense of Article 91 shall be liable only to a disciplinary punishment in respect of this act, even if it is a repeated offence.

A prisoner of war who is recaptured shall be handed over without delay to the competent military authority.

Article 88, fourth paragraph, notwithstanding, prisoners of war punished as a result of an unsuccessful escape may be subjected to special surveillance. Such surveillance must not affect the state of their health, must be undergone in a prisoner of war camp, and must not entail the suppression of any of the safeguards granted them by the present Convention.

ARTICLE 93

Escape or attempt to escape, even if it is a repeated offence, shall not be deemed an aggravating circumstance if the prisoner of war is subjected to trial by judicial proceedings in respect of an offence committed during his escape or attempt to escape.

In conformity with the principle stated in Article 83, offences committed by prisoners of war with the sole intention of facilitating their escape and which do not entail any violence against life or limb, such as offences against public property, theft without intention of self-enrichment, the drawing up or use of false papers, the wearing of civilian clothing, shall occasion disciplinary punishment only.

Prisoners of war who aid or abet an escape or an attempt to escape shall be liable on this count to disciplinary punishment only.

ARTICLE 94

If an escaped prisoner of war is recaptured, the Power on which he depends shall be notified thereof in the manner defined in Article 122, provided notification of his escape has been made.

ARTICLE 95

A prisoner of war accused of an offence against discipline shall not be kept in confinement pending the hearing unless a member of the armed forces of the Detaining Power would be so kept if he were accused of a similar offence, or if it is essential in the interests of camp order and discipline.

Any period spent by a prisoner of war in confinement awaiting the disposal of an offence against discipline shall be reduced to an absolute minimum and shall not exceed fourteen days.

The provisions of Articles 97 and 98 of this Chapter shall apply to prisoners of war who are in confinement awaiting the disposal of offences against discipline.

ARTICLE 96

Acts which constitute offences against discipline shall be investigated immediately.

Without prejudice to the competence of courts and superior military authorities, disciplinary punishment may be ordered only by an officer having disciplinary powers in his capacity as camp commander, or by a responsible officer who replaces him or to whom he has delegated his disciplinary powers.

In no case may such powers be delegated to a prisoner of war or be exercised by a prisoner of war.

Before any disciplinary award is pronounced, the accused shall be given precise information regarding the offences of which he is accused, and given an opportunity of explaining his conduct and of defending himself. He shall be permitted, in particular, to call witnesses and to have recourse, if necessary, to the services of a qualified interpreter. The decision shall be announced to the accused prisoner of war and to the prisoners' representative.

A record of disciplinary punishments shall be maintained by the camp commander and shall be open to inspection by representatives of the Protecting Power.

ARTICLE 97

Prisoners of war shall not in any case be transferred to penitentiary establishments (prisons, penitentiaries, convict prisons, etc.) to undergo disciplinary punishment therein.

All premises in which disciplinary punishments are undergone shall conform to the sanitary requirements set forth in Article 25. A prisoner of war undergoing punishment shall be enabled to keep himself in a state of cleanliness, in conformity with Article 29.

Officers and persons of equivalent status shall not be lodged in the same quarters as non-commissioned officers or men.

Women prisoners of war undergoing disciplinary punishment shall be confined in separate quarters from male prisoners of war and shall be under the immediate supervision of women.

ARTICLE 98

A prisoner of war undergoing confinement as a disciplinary punishment, shall continue to enjoy the benefits of the provisions of this Convention except in so far as these are necessarily rendered inapplicable by the mere fact that he is confined. In no case may he be deprived of the benefits of the provisions of Articles 78 and 126.

A prisoner of war awarded disciplinary punishment may not be deprived of the prerogatives attached to his rank.

Prisoners of war awarded disciplinary punishment shall be allowed to exercise and to stay in the open air at least two hours daily.

They shall be allowed, on their request, to be present at the daily medical inspections. They shall receive the attention which their state of health requires and, if necessary, shall be removed to the camp infirmary or to a hospital.

They shall have permission to read and write, likewise to send and receive letters. Parcels and remittances of money, however, may be withheld from them until the completion of the punishment; they shall meanwhile be entrusted to the prisoners' representative, who will hand over to the infirmary the perishable goods contained in such parcels.

III. JUDICIAL PROCEEDINGS

ARTICLE 99

No prisoner of war may be tried or sentenced for an act which is not forbidden by the law of the Detaining Power or by international law, in force at the time the said act was committed.

No moral or physical coercion may be exerted on a prisoner of war in order to induce him to admit himself guilty of the act of which he is accused.

No prisoner of war may be convicted without having had an opportunity to present his defense and the assistance of a qualified advocate or counsel.

ARTICLE 100

Prisoners of war and the Protecting Powers shall be informed as soon as possible of the offences which are punishable by the death sentence under the laws of the Detaining Power.

Other offences shall not thereafter be made punishable by the death penalty without the concurrence of the Power upon which the prisoners of war depend.

The death sentence cannot be pronounced on a prisoner of war unless the attention of the court has, in accordance with Article 87, second paragraph, been particularly called to the fact that since the accused is not a national of the Detaining Power, he is not bound to it by any duty of allegiance, and that he is in its power as the result of circumstances independent of his own will.

ARTICLE 101

If the death penalty is pronounced on a prisoner of war, the sentence shall not be executed before the expiration of a period of at least six months from the date when the Protecting Power receives, at an indicated address, the detailed communication provided for in Article 107.

ARTICLE 102

A prisoner of war can be validly sentenced only if the sentence has been pronounced by the same courts according to the same procedure as in the case of members of the armed forces of the Detaining Power, and if, furthermore, the provisions of the present Chapter have been observed.

ARTICLE 103

Judicial investigations relating to a prisoner of war shall be conducted as rapidly as circumstances permit and so that his trial shall take place as soon as possible. A prisoner of war shall not be confined while awaiting trial unless a member of the armed forces of the Detaining Power would be so confined if he were accused of a similar offence, or if it is essential to do so in the interests of national security. In no circumstances shall this confinement exceed three months.

Any period spent by a prisoner of war in confinement awaiting trial shall be deducted from any sentence of imprisonment passed upon him and taken into account in fixing any penalty.

The provisions of Articles 97 and 98 of this Chapter shall apply to a prisoner of war whilst in confinement awaiting trial.

ARTICLE 104

In any case in which the Detaining Power has decided to institute judicial proceedings against a prisoner of war, it shall notify the Protecting Power as soon as possible and at least three weeks before the opening of the trial. This period of three weeks shall run as from the day on which such notification reaches the Protecting Power at the address previously indicated by the latter to the Detaining Power.

The said notification shall contain the following information:

1. Surname and first names of the prisoner of war, his rank, his army, regimental, personal or serial number, his date of birth, and his profession or trade, if any;

2. Place of internment or confinement;

3. Specification of the charge or charges on which the prisoner of war is to be arraigned, giving the legal provisions applicable;

4 . Designation of the court which will try the case, likewise the date and place fixed for the opening of the trial.

The same communication shall be made by the Detaining Power to the prisoners' representative.

If no evidence is submitted, at the opening of a trial, that the notification referred to above was received by the Protecting Power, by the prisoner of war and by the prisoners' representative concerned, at least three weeks before the opening of the trial, then the latter cannot take place and must be adjourned.

ARTICLE 105

The prisoner of war shall be entitled to assistance by one of his prisoner comrades, to defense by a qualified advocate or counsel of his own choice, to the calling of witnesses and, if he deems necessary, to the services of a competent interpreter. He shall be advised of these rights by the Detaining Power in due time before the trial.

Failing a choice by the prisoner of war, the Protecting Power shall find him an advocate or counsel, and shall have at least one week at its disposal for the purpose. The Detaining Power shall deliver to the said Power, on request, a list of persons qualified to present the defense. Failing a choice of an advocate or counsel by the prisoner of war or the Protecting Power, the Detaining Power shall appoint a competent advocate or counsel to conduct the defense.

The advocate or counsel conducting the defense on behalf of the prisoner of war shall have at his disposal a period of two weeks at least before the opening of the trial, as well as the necessary facilities to prepare the defense of the accused. He may, in particular, freely visit the accused and interview him in private. He may also confer with any witnesses for the defense, including prisoners of war. He shall have the benefit of these facilities until the term of appeal or petition has expired.

Particulars of the charge or charges on which the prisoner of war is to be arraigned, as well as the documents which are generally communicated to the accused by virtue of the laws in force in the armed forces of the Detaining Power, shall be communicated to the accused prisoner of war in a language which he understands, and in good time before the opening of the trial. The same communication in the same circumstances shall be made to the advocate or counsel conducting the defense on behalf of the prisoner of war.

The representatives of the Protecting Power shall be entitled to attend the trial of the case, unless, exceptionally, this is held in camera in the interest of State security. In such a case the Detaining Power shall advise the Protecting Power accordingly.

ARTICLE 106

Every prisoner of war shall have, in the same manner as the members of the armed forces of the Detaining Power, the right of appeal or petition from any sentence pronounced upon him, with a view to the quashing or revising of the sentence or the reopening of the trial. He shall be fully informed of his right to appeal or petition and of the time limit within which he may do so.

ARTICLE 107

Any judgment and sentence pronounced upon a prisoner of war shall be immediately reported to the Protecting Power in the form of a summary communication, which shall also indicate whether he has the right of appeal with a view to the quashing of the sentence or the reopening of the trial. This communication shall likewise be sent to the prisoners' representative concerned. It shall also be sent to the accused prisoner of war in a language he understands, if the sentence was not pronounced in his presence. The Detaining Power shall also immediately communicate to the Protecting Power the decision of the prisoner of war to use or to waive his right of appeal.

Furthermore, if a prisoner of war is finally convicted or if a sentence pronounced on a prisoner of war in the first instance is a death sentence, the Detaining Power shall as soon as possible address to the Protecting Power a detailed communication containing:

1. The precise wording of the finding and sentence;

2. A summarized report of any preliminary investigation and of the trial, emphasizing in particular the elements of the prosecution and the defense;

3. Notification, where applicable, of the establishment where the sentence will be served.

The communications provided for in the foregoing subparagraphs shall be sent to the Protecting Power at the address previously made known to the Detaining Power.

ARTICLE 108

Sentences pronounced on prisoners of war after a conviction has become duly enforceable, shall be served in the same establishments and under the same conditions as in the case of members of the armed forces of the Detaining Power. These conditions shall in all cases conform to the requirements of health and humanity.

A woman prisoner of war on whom such a sentence has been pronounced shall be confined in separate quarters and shall be under the supervision of women.

In any case, prisoners of war sentenced to a penalty depriving them of their liberty shall retain the benefit of the provisions of Articles 78 and 126 of the present Convention. Furthermore, they shall be entitled to receive and dispatch correspondence, to receive at least one relief parcel monthly, to take regular exercise in the open air, to have the medical care required by their state of health, and the spiritual assistance they may desire. Penalties to which they may be subjected shall be in accordance with the provisions of Article 87, third paragraph.

PART IV TERMINATION OF CAPTIVITY

SECTION I DIRECT REPATRIATION AND ACCOMMODATION IN NEUTRAL COUNTRIES

ARTICLE 109

Subject to the provisions of the third paragraph of this Article, Parties to the conflict are bound to send back to their own country, regardless of number or rank, seriously wounded and seriously sick prisoners of war, after having cared for them until they are fit to travel, in accordance with the first paragraph of the following Article.

Throughout the duration of hostilities, Parties to the conflict shall endeavor, with the cooperation of the neutral Powers concerned, to make arrangements for the accommodation in neutral countries of the sick and wounded prisoners of war referred to in the second paragraph of the following Article. They may, in addition, conclude agreements with a view to the direct repatriation or internment in a neutral country of able-bodied prisoners of war who have undergone a long period of captivity.

No sick or injured prisoner of war who is eligible for repatriation under the first paragraph of this Article, may be repatriated against his will during hostilities.

ARTICLE 110

The following shall be repatriated direct:

1. Incurably wounded and sick whose mental or physical fitness seems to have been gravely diminished.

2. Wounded and sick who, according to medical opinion, are not likely to recover within one year, whose condition requires treatment and whose mental or physical fitness seems to have been gravely diminished.

3. Wounded and sick who have recovered, but whose mental or physical fitness seems to have been gravely and permanently diminished.

The following may be accommodated in a neutral country:

1. Wounded and sick whose recovery may be expected within one year of the date of the wound or the beginning of the illness, if treatment in a neutral country might increase the prospects of a more certain and speedy recovery.

2. Prisoners of war whose mental or physical health, according to medical opinion, is seriously threatened by continued captivity, but whose accommodation in a neutral country might remove such a threat.

The conditions which prisoners of war accommodated in a neutral country must fulfil in order to permit their repatriation shall be fixed, as shall likewise their status, by agreement between the Powers concerned. In general, prisoners of war who have been accommodated in a neutral country, and who belong to the following categories, should be repatriated:

1. Those whose state of health has deteriorated so as to fulfil the conditions laid down for direct repatriation;

2. Those whose mental or physical powers remain, even after treatment, considerably impaired.

If no special agreements are concluded between the Parties to the conflict concerned, to determine the cases of disablement or sickness entailing direct repatriation or accommodation in a neutral country, such cases shall be settled in accordance with the principles laid down in the Model Agreement concerning direct repatriation and accommodation in neutral countries of wounded and sick prisoners of war and in the Regulations concerning Mixed Medical Commissions annexed to the present Convention.

ARTICLE 111

The Detaining Power, the Power on which the prisoners of war depend, and a neutral Power agreed upon by these two Powers, shall endeavor to conclude agreements which will enable prisoners of war to be interned in the territory of the said neutral Power until the close of hostilities.

ARTICLE 112

Upon the outbreak of hostilities, Mixed Medical Commissions shall be appointed to examine sick and wounded prisoners of war, and to make all appropriate decisions regarding them. The appointment, duties and functioning of these Commissions shall be in conformity with the provisions of the Regulations annexed to the present Convention.

However, prisoners of war who, in the opinion of the medical authorities of the Detaining Power, are manifestly seriously injured or seriously sick, may be repatriated without having to be examined by a Mixed Medical Commission.

ARTICLE 113

Besides those who are designated by the medical authorities of the Detaining Power, wounded or sick prisoners of war belonging to the categories listed below shall be entitled to present themselves for examination by the Mixed Medical Commissions provided for in the foregoing Article:

1. Wounded and sick proposed by a physician or surgeon who is of the same nationality, or a national of a Party to the conflict allied with the Power on which the said prisoners depend, and who exercises his functions in the camp.

2. Wounded and sick proposed by their prisoners' representative.

3. Wounded and sick proposed by the Power on which they depend, or by an organization duly recognized by the said Power and giving assistance to the prisoners.

Prisoners of war who do not belong to one of the three foregoing categories may nevertheless present themselves for examination by Mixed Medical Commissions, but shall be examined only after those belonging to the said categories.

The physician or surgeon of the same nationality as the prisoners who present themselves for examination by the Mixed Medical Commission, likewise the prisoners' representative of the said prisoners, shall have permission to be present at the examination.

ARTICLE 114

Prisoners of war who meet with accidents shall, unless the injury is self-inflicted, have the benefit of the provisions of this Convention as regards repatriation or accommodation in a neutral country.

ARTICLE 115

No prisoner of war on whom a disciplinary punishment has been imposed and who is eligible for repatriation or for accommodation in a neutral country, may be kept back on the plea that he has not undergone his punishment.

Prisoners of war detained in connection with a judicial prosecution or conviction and who are designated for repatriation or accommodation in a neutral country, may benefit by such measures before the end of the proceedings or the completion of the punishment, if the Detaining Power consents.

Parties to the conflict shall communicate to each other the names of those who will be detained until the end of the proceedings or the completion of the punishment.

ARTICLE 116

The costs of repatriating prisoners of war or of transporting them to a neutral country shall be borne, from the frontiers of the Detaining Power, by the Power on which the said prisoners depend.

ARTICLE 117

No repatriated person may be employed on active military service.

SECTION II RELEASE AND REPATRIATION OF PRISONERS OF WAR AT THE CLOSE OF HOSTILITIES

ARTICLE 118

Prisoners of war shall be released and repatriated without delay after the cessation of active hostilities.

In the absence of stipulations to the above effect in any agreement concluded between the Parties to the conflict with a view to the cessation of hostilities, or failing any such agreement, each of the Detaining Powers shall itself establish and execute without delay a plan of repatriation in conformity with the principle laid down in the foregoing paragraph.

In either case, the measures adopted shall be brought to the knowledge of the prisoners of war.

The costs of repatriation of prisoners of war shall in all cases be equitably apportioned between the Detaining Power and the Power on which the prisoners depend. This apportionment shall be carried out on the following basis:

(a) If the two Powers are contiguous, the Power on which the prisoners of war depend shall bear the costs of repatriation from the frontiers of the Detaining Power.

(b) If the two Powers are not contiguous, the Detaining Power shall bear the costs of transport of prisoners of war over its own territory as far as its frontier or its port of embarkation nearest to the territory of the Power on which the prisoners of war depend. The Parties concerned shall agree between themselves as to the equitable apportionment of the remaining costs of the repatriation. The conclusion of this agreement shall in no circumstances justify any delay in the repatriation of the prisoners of war.

ARTICLE 119

Repatriation shall be effected in conditions similar to those laid down in Articles 46 to 48 inclusive of the present Convention for the transfer of prisoners of war, having regard to the provisions of Article 118 and to those of the following paragraphs.

On repatriation, any articles of value impounded from prisoners of war under Article 18, and any foreign currency which has not been converted into the currency of the Detaining Power, shall be restored to them. Articles of value and foreign currency which, for any reason whatever, are not restored to prisoners of war on repatriation, shall be dispatched to the Information Bureau set up under Article 122.

Prisoners of war shall be allowed to take with them their personal effects, and any correspondence and parcels which have arrived for them. The weight of such baggage may be limited, if the conditions of repatriation so require, to what each prisoner can reasonably carry. Each prisoner shall in all cases be authorized to carry at least twenty-five kilograms.

The other personal effects of the repatriated prisoner shall be left in the charge of the Detaining Power which shall have them forwarded to him as soon as it has concluded an agreement to this effect, regulating the conditions of transport and the payment of the costs involved, with the Power on which the prisoner depends.

Prisoners of war against whom criminal proceedings for an indictable offence are pending may be detained until the end of such proceedings, and, if necessary, until the completion of the punishment. The same shall apply to prisoners of war already convicted for an indictable offence.

Parties to the conflict shall communicate to each other the names of any prisoners of war who are detained until the end of the proceedings or until punishment has been completed.

By agreement between the Parties to the conflict, commissions shall be established for the purpose of searching for dispersed prisoners of war and of assuring their repatriation with the least possible delay.

SECTION III DEATH OF PRISONERS OF WAR

ARTICLE 120

Wills of prisoners of war shall be drawn up so as to satisfy the conditions of validity required by the legislation of their country of origin, which will take steps to inform the Detaining Power of its requirements in this respect. At the request of the prisoner of war and, in all cases, after death, the will shall be transmitted without delay to the Protecting Power; a certified copy shall be sent to the Central Agency.

Death certificates in the form annexed to the present Convention, or lists certified by a responsible officer, of all persons who die as prisoners of war shall be forwarded as rapidly as possible to the Prisoner of War Information Bureau established in accordance with Article 122. The death certificates or certified lists shall show particulars of identity as set out in the third paragraph of Article 17, and also the date and place of death, the cause of death, the date and place of burial and all particulars necessary to identify the graves.

The burial or cremation of a prisoner of war shall be preceded by a medical examination of the body with a view to confirming death and enabling a report to be made and, where necessary, establishing identity.

The detaining authorities shall ensure that prisoners of war who have died in captivity are honorably buried, if possible according to the rites of the religion to which they belonged, and that their graves are respected, suitably maintained and marked so as to be found at any time. Wherever possible, deceased prisoners of war who depended on the same Power shall be interred in the same place.

Deceased prisoners of war shall be buried in individual graves unless unavoidable circumstances require the use of collective graves. Bodies may be cremated only for imperative reasons of hygiene, on account of the religion of the deceased or in accordance with his express wish to this effect. In case of cremation, the fact shall be stated and the reasons given in the death certificate of the deceased.

In order that graves may always be found, all particulars of burials and graves shall be recorded with a Graves Registration Service established by the Detaining Power. Lists of graves and particulars of the prisoners of war interred in cemeteries and elsewhere shall be transmitted to the Power on which such prisoners of war depended. Responsibility for the care of these graves and for records of any subsequent moves of the bodies shall rest on the Power controlling the territory, if a Party to the present Convention. These provisions shall also apply to the ashes, which shall be kept by the Graves Registration Service until proper disposal thereof in accordance with the wishes of the home country.

ARTICLE 121

Every death or serious injury of a prisoner of war caused or suspected to have been caused by a sentry, another prisoner of war, or any other person, as well as any death the cause of which is unknown, shall be immediately followed by an official enquiry by the Detaining Power.

A communication on this subject shall be sent immediately to the Protecting Power. Statements shall be taken from witnesses, especially from those who are prisoners of war, and a report including such statements shall be forwarded to the Protecting Power.

If the enquiry indicates the guilt of one or more persons, the Detaining Power shall take all measures for the prosecution of the person or persons responsible.

PART V INFORMATION BUREAU AND RELIEF SOCIETIES FOR PRISONERS OF WAR

ARTICLE 122

Upon the outbreak of a conflict and in all cases of occupation, each of the Parties to the conflict shall institute an official Information Bureau for prisoners of war who are in its power. Neutral or non-belligerent Powers who may have received within their territory persons belonging to one of the categories referred to in Article 4, shall take the same action with respect to such persons. The Power concerned shall ensure that the Prisoners of War Information Bureau is provided with the necessary accommodation, equipment and staff to ensure its efficient working. It shall be at liberty to employ prisoners of war in such a Bureau under the conditions laid down in the Section of the present Convention dealing with work by prisoners of war.

Within the shortest possible period, each of the Parties to the conflict shall give its Bureau the information referred to in the fourth, fifth and sixth paragraphs of this Article regarding any enemy person belonging to one of the categories referred to in Article 4, who has fallen into its power. Neutral or non-belligerent Powers shall take the same action with regard to persons belonging to such categories whom they have received within their territory.

The Bureau shall immediately forward such information by the most rapid means to the Powers concerned, through the intermediary of the Protecting Powers and likewise of the Central Agency provided for in Article 123.

This information shall make it possible quickly to advise the next of kin concerned. Subject to the provisions of Article 17, the information shall include, in so far as available to the Information Bureau, in respect of each prisoner of war, his surname, first names, rank, army, regimental, personal or serial number, place and full date of birth, indication of the Power on which he depends, first name of the father and maiden name of the mother, name and address of the person to be informed and the address to which correspondence for the prisoner may be sent.

The Information Bureau shall receive from the various departments concerned information regarding transfers, releases, repatriations, escapes, admissions to hospital, and deaths, and shall transmit such information in the manner described in the third paragraph above.

Likewise, information regarding the state of health of prisoners of war who are seriously ill or seriously wounded shall be supplied regularly, every week if possible.

The Information Bureau shall also be responsible for replying to all inquiries sent to it concerning prisoners of war, including those who have died in captivity; it will make any inquiries necessary to obtain the information which is asked for if this is not in its possession.

All written communications made by the Bureau shall be authenticated by a signature or a seal.

The Information Bureau shall furthermore be charged with collecting all personal valuables, including sums in currencies other than that of the Detaining Power and documents of importance to the next of kin, left by prisoners of war who have been repatriated or released, or who have escaped or died, and shall forward the said valuables to the Powers concerned. Such articles shall be sent by the Bureau in sealed packets which shall be accompanied by statements giving clear and full particulars of the identity of the person to whom the articles belonged, and by a complete list of the contents of the parcel. Other personal effects of such prisoners of war shall be transmitted under arrangements agreed upon between the Parties to the conflict concerned.

ARTICLE 123

A Central Prisoners of War Information Agency shall be created in a neutral country. The International Committee of the Red Cross shall, if it deems necessary, propose to the Powers concerned the organization of such an Agency.

The function of the Agency shall be to collect all the information it may obtain through official or private channels respecting prisoners of war, and to transmit it as rapidly as possible to the country of origin of the prisoners of war or to the Power on which they depend. It shall receive from the Parties to the conflict all facilities for effecting such transmissions.

The High Contracting Parties, and in particular those whose nationals benefit by the services of the Central Agency, are requested to give the said Agency the financial aid it may require.

The foregoing provisions shall in no way be interpreted as restricting the humanitarian activities of the International Committee of the Red Cross, or of the relief Societies provided for in Article 125.

ARTICLE 124

The national Information Bureau and the Central Information Agency shall enjoy free postage for mail, likewise all the exemptions provided for in Article 74, and further, so far as possible, exemption from telegraphic charges or, at least, greatly reduced rates.

ARTICLE 125

Subject to the measures which the Detaining Powers may consider essential to ensure their security or to meet any other reasonable need, the representatives of religious organizations, relief societies, or any other organization assisting prisoners of war, shall receive from the said Powers, for themselves and their duly accredited agents, all necessary facilities for visiting the prisoners, distributing relief supplies and material, from any source, intended for religious, educational or recreative purposes, and for assisting them in organizing their leisure time within the camps. Such societies or organizations may be constituted in the territory of the Detaining Power or in any other country, or they may have an international character.

The Detaining Power may limit the number of societies and organizations whose delegates are allowed to carry out their activities in its territory and under its supervision, on condition, however, that such limitation shall not hinder the effective operation of adequate relief to all prisoners of war.

The special position of the International Committee of the Red Cross in this field shall be recognized and respected at all times.

As soon as relief supplies or material intended for the above-mentioned purposes are handed over to prisoners of war, or very shortly afterwards, receipts for each consignment, signed by the prisoners' representative, shall be forwarded to the relief society or organization making the shipment. At the same time, receipts for these consignments shall be supplied by the administrative authorities responsible for guarding the prisoners.

PART VI EXECUTION OF THE CONVENTION

SECTION I GENERAL PROVISIONS

ARTICLE 126

Representatives or delegates of the Protecting Powers shall have permission to go to all places where prisoners of war may be, particularly to places of internment, imprisonment and labor, and shall have access to all premises occupied by prisoners of war; they shall also be allowed to go to the places of departure, passage and arrival of prisoners who are being transferred. They shall be able to interview the prisoners, and in particular the prisoners' representatives, without witnesses, either personally or through an interpreter.

Representatives and delegates of the Protecting Powers shall have full liberty to select the places they wish to visit. The duration and frequency of these visits shall not be restricted. Visits may not be prohibited except for reasons of imperative military necessity, and then only as an exceptional and temporary measure.

The Detaining Power and the Power on which the said prisoners of war depend may agree, if necessary, that compatriots of these prisoners of war be permitted to participate in the visits.

The delegates of the International Committee of the Red Cross shall enjoy the same prerogatives. The appointment of such delegates shall be submitted to the approval of the Power detaining the prisoners of war to be visited.

ARTICLE 127

The High Contracting Parties undertake, in time of peace as in time of war, to disseminate the text of the present Convention as widely as possible in their respective countries, and, in particular, to include the study thereof in their programs of military and, if possible, civil instruction, so that the principles thereof may become known to all their armed forces and to the entire population.

Any military or other authorities, who in time of war assume responsibilities in respect of prisoners of war, must possess the text of the Convention and be specially instructed as to its provisions.

ARTICLE 128

The High Contracting Parties shall communicate to one another through the Swiss Federal Council and, during hostilities, through the Protecting Powers, the official translations of the

present Convention, as well as the laws and regulations which they may adopt to ensure the application thereof.

ARTICLE 129

The High Contracting Parties undertake to enact any legislation necessary to provide effective penal sanctions for persons committing, or ordering to be committed, any of the grave breaches of the present Convention defined in the following Article.

Each High Contracting Party shall be under the obligation to search for persons alleged to have committed, or to have ordered to be committed, such grave breaches, and shall bring such persons, regardless of their nationality, before its own courts. It may also, if it prefers, and in accordance with the provisions of its own legislation, hand such persons over for trial to another High Contracting Party concerned, provided such High Contracting Party has made out a prima facie case.

Each High Contracting Party shall take measures necessary for the suppression of all acts contrary to the provisions of the present Convention other than the grave breaches defined in the following Article.

In all circumstances, the accused persons shall benefit by safeguards of proper trial and defense, which shall not be less favorable than those provided by Article 105 and those following of the present Convention.

ARTICLE 130

Grave breaches to which the preceding Article relates shall be those involving any of the following acts, if committed against persons or property protected by the Convention: willful killing, torture or inhuman treatment, including biological experiments, willfully causing great suffering or serious injury to body or health, compelling a prisoner of war to serve in the forces of the hostile Power, or willfully depriving a prisoner of war of the rights of fair and regular trial prescribed in this Convention.

ARTICLE 131

No High Contracting Party shall be allowed to absolve itself or any other High Contracting Party of any liability incurred by itself or by another High Contracting Party in respect of breaches referred to in the preceding Article.

ARTICLE 132

At the request of a Party to the conflict, an enquiry shall be instituted, in a manner to be decided between the interested Parties, concerning any alleged violation of the Convention.

If agreement has not been reached concerning the procedure for the enquiry, the Parties should agree on the choice of an umpire who will decide upon the procedure to be followed.

Once the violation has been established, the Parties to the conflict shall put an end to it and shall repress it with the least possible delay.

SECTION II FINAL PROVISIONS

ARTICLE 133

The present Convention is established in English and in French. Both texts are equally authentic. The Swiss Federal Council shall arrange for official translations of the Convention to be made in the Russian and Spanish languages.

ARTICLE 134

The present Convention replaces the Convention of 27 July 1929, in relations between the High Contracting Parties.

ARTICLE 135

In the relations between the Powers which are bound by The Hague Convention respecting the Laws and Customs of War on Land, whether that of July 29, 1899, or that of October 18, 1907, and which are parties to the present Convention, this last Convention shall be complementary to Chapter II of the Regulations annexed to the above-mentioned Conventions of The Hague.

ARTICLE 136

The present Convention, which bears the date of this day, is open to signature until February 12, 1950, in the name of the Powers represented at the Conference which opened at Geneva on April 21, 1949; furthermore, by Powers not represented at that Conference, but which are parties to the Convention of July 27, 1929.

ARTICLE 137

The present Convention shall be ratified as soon as possible and the ratifications shall be deposited at Berne.

A record shall be drawn up of the deposit of each instrument of ratification and certified copies of this record shall be transmitted by the Swiss Federal Council to all the Powers in whose name the Convention has been signed, or whose accession has been notified.

ARTICLE 138

The present Convention shall come into force six months after not less than two instruments of ratification have been deposited.

Thereafter, it shall come into force for each High Contracting Party six months after the deposit of the instrument of ratification.

ARTICLE 139

From the date of its coming into force, it shall be open to any Power in whose name the present Convention has not been signed, to accede to this Convention.

ARTICLE 140

Accessions shall be notified in writing to the Swiss Federal Council, and shall take effect six months after the date on which they are received.

The Swiss Federal Council shall communicate the accessions to all the Powers in whose name the Convention has been signed, or whose accession has been notified.

ARTICLE 141

The situations provided for in Articles 2 and 3 shall give immediate effect to ratifications deposited and accessions notified by the Parties to the conflict before or after the beginning of hostilities or occupation. The Swiss Federal Council shall communicate by the quickest method any ratifications or accessions received from Parties to the conflict.

ARTICLE 142

Each of the High Contracting Parties shall be at liberty to denounce the present Convention.

The denunciation shall be notified in writing to the Swiss Federal Council, which shall transmit it to the Governments of all the High Contracting Parties.

The denunciation shall take effect one year after the notification thereof has been made to the Swiss Federal Council. However, a denunciation of which notification has been made at a time when the denouncing Power is involved in a conflict shall not take effect until peace has been concluded, and until after operations connected with the release and repatriation of the persons protected by the present Convention have been terminated.

The denunciation shall have effect only in respect of the denouncing Power. It shall in no way impair the obligations which the Parties to the conflict shall remain bound to fulfill by virtue of the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity and the dictates of the public conscience.

ARTICLE 143

The Swiss Federal Council shall register the present Convention with the Secretariat of the United Nations. The Swiss Federal Council shall also inform the Secretariat of the United Nations of all ratifications, accessions and denunciations received by it with respect to the present Convention.

IN WITNESS WHEREOF the undersigned, having deposited their respective full powers, have signed the present Convention.

DONE at Geneva this twelfth day of August 1949, in the English and French languages. The original shall be deposited in the Archives of the Swiss Confederation. The Swiss Federal Council shall transmit certified copies thereof to each of the signatory and acceding States.

SECTION II. GENEVA CONVENTIONS RELATIVE TO THE PROTECTION OF CIVILIAN PERSONS IN TIME OF WAR (FOURTH GENEVA CONVENTION)

The following excerpted articles from the Geneva Conventions contain requirements concerning the treatment of civilians during time of war. Violations of these articles can constitute war crimes and should be treated as such.

PART I

GENERAL PROVISIONS

Article 1

The High Contracting Parties undertake to respect and to ensure respect for the present Convention in all circumstances.

Article 2

In addition to the provisions which shall be implemented in peacetime, the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them.

The Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance.

Although one of the Powers in conflict may not be a party to the present Convention, the Powers who are parties thereto shall remain bound by it in their mutual relations. They shall furthermore be bound by the Convention in relation to the said Power, if the latter accepts and applies the provisions thereof.

Article 3

In the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties, each Party to the conflict shall be bound to apply, as a minimum, the following provisions:

1. Persons taking no active part in the hostilities, including members of armed forces who have laid down their arms and those placed hors de combat by sickness, wounds, detention, or any other cause, shall in all circumstances be treated humanely, without any adverse distinction founded on race, colour, religion or faith, sex, birth or wealth, or any other similar criteria.

To this end, the following acts are and shall remain prohibited at any time and in any place whatsoever with respect to the above-mentioned persons:

(a) Violence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture;

(b) Taking of hostages;

(c) Outrages upon personal dignity, in particular humiliating and degrading treatment;

(d) The passing of sentences and the carrying out of executions without previous judgment pronounced by a regularly constituted court, affording all the judicial guarantees which are recognized as indispensable by civilized peoples.

2. The wounded and sick shall be collected and cared for.

An impartial humanitarian body, such as the International Committee of the Red Cross, may offer its services to the Parties to the conflict.

The Parties to the conflict should further endeavour to bring into force, by means of special agreements, all or part of the other provisions of the present Convention.

The application of the preceding provisions shall not affect the legal status of the Parties to the conflict.

Article 4

Persons protected by the Convention are those who, at a given moment and in any manner whatsoever, find themselves, in case of a conflict or occupation, in the hands of a Party to the conflict or Occupying Power of which they are not nationals.
Nationals of a State which is not bound by the Convention are not protected by it.

Nationals of a neutral State who find themselves in the territory of a belligerent State, and nationals of a co-belligerent State, shall not be regarded as protected persons while the State of which they are nationals has normal diplomatic representation in the State in whose hands they are.

The provisions of Part II are, however, wider in application, as defined in Article 13.

Persons protected by the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of August 12, 1949, or by the Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea of August 12, 1949, or by the Geneva Convention relative to the Treatment of Prisoners of War of August 12, 1949, shall not be considered as protected persons within the meaning of the present Convention.

Article 5

Where, in the territory of a Party to the conflict, the latter is satisfied that an individual protected person is definitely suspected of or engaged in activities hostile to the security of the State, such individual person shall not be entitled to claim such rights and privileges under the present Convention as would, if exercised in the favour of such individual person, be prejudicial to the security of such State.

Where in occupied territory an individual protected person is detained as a spy or saboteur, or as a person under definite suspicion of activity hostile to the security of the Occupying Power, such person shall, in those cases where absolute military security so requires, be regarded as having forfeited rights of communication under the present Convention.

In each case, such persons shall nevertheless be treated with humanity, and in case of trial, shall not be deprived of the rights of fair and regular trial prescribed by the present Convention. They shall also be granted the full rights and privileges of a protected person under the present Convention at the earliest date consistent with the security of the State or Occupying Power, as the case may be.

Article 25

All persons in the territory of a Party to the conflict, or in a territory occupied by it, shall be enabled to give news of a strictly personal nature to members of their families, wherever they may be, and to receive news from them. This correspondence shall be forwarded speedily and without undue delay.

If, as a result of circumstances, it becomes difficult or impossible to exchange family correspondence by the ordinary post, the Parties to the conflict concerned shall apply to a neutral intermediary, such as the Central Agency provided for in Article 140, and shall decide in consultation with it how to ensure the fulfillment of their obligations under the best possible conditions, in particular with the cooperation of the National Red Cross (Red Crescent, Red Lion and Sun) Societies.

If the Parties to the conflict deem it necessary to restrict family correspondence, such restrictions shall be confined to the compulsory use of standard forms containing twenty-five freely chosen words, and to the limitation of the number of these forms dispatched to one each month.

PART III

STATUS AND TREATMENT OF PROTECTED PERSONS

SECTION I

PROVISIONS COMMON TO THE TERRITORIES OF THE PARTIES
TO THE CONFLICT AND TO OCCUPIED TERRITORIES

Article 27

Protected persons are entitled, in all circumstances, to respect for their persons, their honour, their family rights, their religious convictions and practices, and their manners and customs. They shall at all times be humanely treated, and shall be protected especially against all acts of violence or threats thereof and against insults and public curiosity.

Women shall be especially protected against any attack on their honour, in particular against rape, enforced prostitution, or any form of indecent assault.

Without prejudice to the provisions relating to their state of health, age and sex, all protected persons shall be treated with the same consideration by the Party to the conflict in whose power they are, without any adverse distinction based, in particular, on race, religion or political opinion.

However, the Parties to the conflict may take such measures of control and security in regard to protected persons as may be necessary as a result of the war.

Article 28

The presence of a protected person may not be used to render certain points or areas immune from military operations.

Article 29

The Party to the conflict in whose hands protected persons may be is responsible for the treatment accorded to them by its agents, irrespective of any individual responsibility which may be incurred.

Article 30

Protected persons shall have every facility for making application to the Protecting Powers, the International Committee of the Red Cross, the National Red Cross (Red Crescent, Red Lion and Sun) Society of the country where they may be, as well as to any organization that might assist them.

These several organizations shall be granted all facilities for that purpose by the authorities, within the bounds set by military or security considerations.

Apart from the visits of the delegates of the Protecting Powers and of the International Committee of the Red Cross, provided for by Article 143, the Detaining or Occupying Powers shall facilitate as much as possible visits to protected persons by the representatives of other organizations whose object is to give spiritual aid or material relief to such persons.

Article 31

No physical or moral coercion shall be exercised against protected persons, in particular to obtain information from them or from third parties.

Article 32

The High Contracting Parties specifically agree that each of them is prohibited from taking any measure of such a character as to cause the physical suffering or extermination of protected persons in their hands. This prohibition applies not only to murder, torture, corporal punishment, mutilation and medical or scientific experiments not necessitated by the medical treatment of a protected person but also to any other measures of brutality whether applied by civilian or military agents.

Article 33

No protected person may be punished for an offence he or she has not personally committed. Collective penalties and likewise all measures of intimidation or of terrorism are prohibited.

Pillage is prohibited.

Reprisals against protected persons and their property are prohibited.

Article 34

The taking of hostages is prohibited.

SECTION II

ALIENS IN THE TERRORITY OF A PARTY TO THE CONFLICT

Article 41

Should the Power in whose hands protected persons may be consider the measures of control mentioned in the present Convention to be inadequate, it may not have recourse to any other measure of control more severe than that of assigned residence or internment, in accordance with the provisions of Articles 42 and 43.

In applying the provisions of Article 39, second paragraph, to the cases of persons required to leave their usual places of residences by virtue of a decision placing them in assigned residence elsewhere, the Detaining Power shall be guided as closely as possible by the standards of welfare set forth in Part III, Section IV of this Convention.

Article 42

The internment or placing in assigned residence of protected persons may be ordered only if the security of the Detaining Power makes it absolutely necessary.

If any person, acting through the representatives of the Protecting Power, voluntarily demands internment, and if his situation renders this step necessary, he shall be interned by the Power in whose hands he may be.

Article 43

Any protected person who has been interned or placed in assigned residence shall be entitled to have such action reconsidered as soon as possible by an appropriate court or administrative board designated by the Detaining Power for that purpose. If the internment or placing in assigned residence is maintained, the court or administrative board shall periodically, and at least twice yearly, give consideration to his or her case, with a view to the favourable amendment of the initial decision, if circumstances permit.

Unless the protected persons concerned object, the Detaining Power shall, as rapidly as possible, give the Protecting Power the names of any protected persons who have been interned or subjected to assigned residence, or who have been released from internment or assigned residence. The decisions of the courts or boards mentioned in the first paragraph of the present Article shall also, subject to the same conditions, be notified as rapidly as possible to the Protecting Power.

Article 44

In applying the measures of control mentioned in the present Convention, the Detaining Power shall not treat as enemy aliens exclusively on the basis of their nationality de jure of an enemy State, refugees who do not, in fact, enjoy the protection of any government.

Appendix B

Source and Information Reliability Matrix

SOURCE RELIABILITY

B-1. Reliability ratings range from "Reliable" (A) to "Unreliable" (E) as shown in Table B-1. In every instance the rating is based on previous reporting from that source. If there has been no previous reporting, the source must be rated as "F". [NOTE: An "F" rating does not necessarily mean that the source cannot be trusted, but that there is no reporting history and therefore no basis for making a determination.]

Table B-1. Evaluation of Source Reliability.

A	**Reliable**	**No doubt** of authenticity, trustworthiness, or competency; has a history of complete reliability
B	**Usually Reliable**	**Minor doubt** about authenticity, trustworthiness, or competency; has a history of valid information most of the time
C	**Fairly Reliable**	**Doubt** of authenticity, trustworthiness, or competency but has provided valid information in the past
D	**Not Usually Reliable**	**Significant doubt** about authenticity, trustworthiness, or competency but has provided valid information in the past
E	**Unreliable**	**Lacking** in authenticity, trustworthiness, and competency; history of invalid information
F	**Cannot Be Judged**	**No basis** exists for evaluating the reliability of the source

INFORMATION CONTENT

B-2. The highest degree of confidence in reported information is given to that which has been confirmed by outside sources, "1". Table B-2 shows evaluation of information content. The degree of confidence decreases if the information is not confirmed, and/or does not seem to make sense. The lowest evaluated rating of "5" means that the information is considered to be false. [NOTE: A rating of "6" does not necessarily mean false information, but is generally used to indicate that no determination can be made since the information is completely new.]

Table B-2. Evaluation of Information Content.

1	**Confirmed**	**Confirmed** by other independent sources; **logical** in itself; **Consistent** with other information on the subject
2	**Probably True**	Not confirmed; **logical** in itself; **consistent** with other information on the subject
3	**Possibly True**	Not confirmed; **reasonably logical** in itself; **agrees with some** other information on the subject
4	**Doubtfully True**	Not confirmed; possible but **not logical**; **no other information** on the subject
5	**Improbable**	Not confirmed; **not logical** in itself; **contradicted** by other information on the subject
6	**Cannot Be Judged**	**No basis** exists for evaluating the validity of the information

Appendix C

Pre-Deployment Planning

HUMINT leaders must anticipate, identify, consider, and evaluate all potential threats. They must take advantage of enhanced information flow through hierarchical and nonhierarchical networks (computer, communications, and personnel). HCTs should—

- Review available databases on assigned contingency AOIs; review existing IPB products, conduct IPB on these AOIs; and develop appropriate IPB products. Information on databases created for specific contingencies can be gotten from the J2X.
- Continually monitor and update their OPLANs to reflect the evolving situation.
- Be aware of higher headquarters SOPs and DIA manuals for specific ISR management guidance.
- Prepare and practice an intelligence "surge" on likely contingency crises.
- Prepare and practice coordination from pre-deployment through redeployment with personnel from HUMINT, IMINT, MASINT, SIGINT, CA, PSYOP, SOF units, MP, and Engineers.
- Plan for requirements to support 24-hour operations: automation, communications capacity, and personnel necessary to provide continuous intelligence information collection and RM, processing, and reporting.
- Plan and coordinate for linguistic support.
- Forward all RFIs to higher headquarters in accordance with SOPs.
- Prepare and practice coordination with units they will support during pre-deployment exercises. Liaison must be conducted with commanders, S2s, administrative support personnel, logistical support personnel, communications personnel, and others. Obtain supported unit's briefing slide formats.
- Obtain copies of the supported unit's SOPs and ensure all team members are aware of the procedures governing HUMINT interface.
- Ensure that team data processing equipment is compatible with the supported unit's network structure and that appropriate interfaces are available.
- Exercise unit deployment SOPs, load plans, and packing lists.

Helpful Unclassified Links:

- https://portal.rccb.osis.gov/index.jsp Foreign Broadcast Information Service home page.
- http://wnc.fedworld.gov/ International news compiled by the US Department of Commerce.

- http://www.state.gov/s/inr/ Department of State's Bureau of Intelligence and Research home page. Contains country and region-specific information, policies, and warnings.
- http://ebird.afis.osd.mil/ Early Bird News Service of the Armed Forces Information Service.
- http://164.214.2.59/ National Geospatial-Intelligence Agency (NGA) (formerly National Imagery and Mapping Agency).
- http://memory.loc.gov/frd/cs/cshome.html#toc Country Studies from the Federal Research Division of the Library of Congress.

Appendix D

S2 Guide for Handling Detainees, Captured Enemy Documents, and Captured Enemy Equipment

D-1. Detainees, retained personnel, CEDs, and CEE are critical sources of combat intelligence. Often the Maneuver Battalion S2 is the first MI officer to encounter these sources. His actions are critical to the exploitation system. Information from these items is time sensitive, and these information sources need to be exploited at as low an echelon as possible. The S2 should anticipate requirements for support based on planned missions and request HUMINT collector support as necessary. If unable to receive HUMINT collector support, the S2 must be prepared to exploit these sources of information to the best of his ability and more importantly expedite their evacuation to locations and units where they can be exploited.

PURPOSE

D-2. This guide is for battalion and brigade S2s. It explains standard procedures on what the S2 should do when his unit—

- Captures an enemy soldier or other detainee.
- Encounters a civilian on the battlefield.
- Finds or captures an enemy document.
- Discovers an unusual enemy weapon or other unusual piece of equipment during tactical operations.

PERSONNEL HANDLING

D-3. The GPW defines persons entitled to treatment as prisoners of war upon capture, in Article 4 (see Appendix A, Section I).

D-4. The GC defines the civilian population (exclusive of those civilian persons listed in GPW, Article 4) who benefit to varying degrees from the provisions of the Geneva Conventions. (See Appendix A, Sections II and III.)

D-5. Persons in each of these categories have distinct rights, duties, and restrictions. Persons who are not members of the Armed Forces, as defined in Article 4, GPW, who bear arms or engage in other conduct hostile to the enemy thereby deprive themselves of many of the privileges attaching to the members of the civilian population. The capturing unit treats all combatants and noncombatants who are suspected of being part of the threat force as EPWs or retained personnel until their status can be determined. This determination normally occurs at the detainee collection point or at a higher echelon. Noncombatants are handled, questioned, detained, evacuated, and released in accordance with theater policy. In all cases, detainees are treated humanely.

D-6. Detainees are treated humanely but with firmness at all times. High standards of discipline are required not only of detainees but also of capturing and escort forces. Fraternization with detainees or mistreatment or abuse of them is not only a violation but also is not conducive to good discipline. In addition to not being conducive to good discipline, the mistreatment or abuse of detainees is a violation of the UCMJ for which violators may be punished. The control of detainees is exercised through the issuance and firm enforcement of necessary instructions in their own language. Instructions relating to their control during evacuation from the combat zone should be as brief as possible. Care must be taken to ensure that detainees have a clear understanding of all instructions to them.

D-7. At the capture point, the capturing element performs the following steps on detainees. The senior soldier will ensure that the steps are performed. The steps are referred to as the "Five S's and a T".

STEP 1. SEARCH

D-8. The capturing unit's first job is to disarm, search, and maintain positive control over all detainees. The detainees are disarmed and searched for concealed weapons and for equipment and documents of particular intelligence value immediately upon capture, unless the number of detainees captured, enemy action, or other circumstances make such a search impracticable. Until each detainee is searched, the responsible forces must be alert to prevent the use of concealed weapons or destruction of documents or equipment.

D-9. The capturing unit gathers all loose CEDs and CEE in the area. Identification documents and protective military equipment such as helmets or NBC gear stay with the detainee unless otherwise directed by the battalion S2.

- Equipment. Items of personal or individual equipment that are new or appear to be of a type not previously observed may be of intelligence value and should be processed and reported in accordance with the unit's SOP, specific evacuation instructions in Annex B (Intelligence) of the OPORD, and theater policy. Equipment for personal protection such as protective masks or protective clothing may not be taken unless replaced with equivalent equipment.
- Documents. A CED is any piece of recorded information that has been in the hands of the enemy. CEDs include but are not limited to maps, sketches, photographs, orders, tactical and technical manuals and instructions, code books, log books, maintenance records, shipping and packing slips and lists, war and field diaries, personal diaries, pay books, newspapers, service records, postal savings books, payrolls, postcards and letters, and any written, printed, engraved, or photographic matter that may contain information relative to the enemy and to weather and terrain data. A capturing unit is normally not able to accurately determine the potential intelligence value of any documents found on the detainee. It is therefore normally expedient to remove all documents, with the exception of the detainee's primary identification document. These documents are sealed in a waterproof

container and tagged with part C of the capture tag. If capture tags are not available, the document bag must be marked at a minimum to identify the detainee to whom the documents belong (see Appendix I).

- Personal effects. Except as provided in Step 1, detainees should be permitted to retain all of their personal effects including money; valuables; protective equipment, such as helmets, protective masks, and like items; effects and articles used for clothing or eating, except knives and forks; identification cards or tags; badges of grade and nationality; and articles having a personal or sentimental value. When items of equipment issued for the personal protection of detainees are taken from them, they must be replaced with equivalent items serving the same purpose. Although money and other valuables may be taken from detainees as a security measure, they must then be receipted for and a record thereof maintained in a special register. These administrative steps normally are not practical to accomplish prior to arrival of the detainee at an EPW camp.

STEP 2. SILENCE

D-10. Detainees are kept silent so that they cannot plan deception or encourage each other to resist. Keeping the detainees silent also prevents them from relieving the stress and shock of capture by talking with others. If the shock of capture is preserved, HUMINT collectors can take advantage of it in an approach. The capturing unit instructs or signals the detainees to be silent. If that does not work, the detainee is gagged. Guards give orders to detainees, but do not converse with them or give them any comfort items.

STEP 3. SAFEGUARD

D-11. All detainees are promptly evacuated out of the "danger" zone. Their presence may not be used to render points or areas immune to attack, nor should they be retained for participation in psychological warfare or other activities. The capturing forces must protect detainees from reprisals. Detainees will not be denied food, potable water, or appropriate clothing and shelter. Necessary medical attention will not be delayed. Those detainees held in an area should be provided protective facilities and equipment and should be oriented as to procedures to be followed in case of chemical, biological, and radiological agent attack.

STEP 4. SEGREGATE

D-12. The capturing unit separates officers from enlisted, senior from junior, male from female, and civilian from military within their capabilities to both guard and safeguard the detainees. (Physical segregation at this point is not always possible.) Deserters and people of different nationalities and ideologies should be further segregated. The capturing unit prepares a capture tag and puts one on each detainee (see Figure D-1). Tagging procedures are discussed in paragraph D-16.

STEP 5. SPEED TO THE REAR

D-13. The capturing unit moves detainees and CEDs to the unit supply point or other area where transportation to the rear is available for evacuation. Evacuation of detainees from the combat zone should be effected within the minimum time after capture. While in the combat zone, not only may detainees become casualties as the result of enemy fire but also the fluidity of operations, the wide dispersion of units, and the austerity of facilities may necessitate their rapid evacuation.

D-14. The normal evacuation channel is from the detainee collection point through intermediate detainee holding areas to an internment facility at a higher echelon. Available returning transportation, however, may bypass any intermediate detainee holding area and proceed directly to a corps or theater internment facility. Detainees will then be processed directly into the corps or theater internment facility. Evacuation may be by foot, vehicle, rail, aircraft, or ship. Evacuate detainees who are litter patients through medical channels.

D-15. The command (brigade and above) from which the detainees are being evacuated is responsible to provide transportation and rations and for coordinating all other matters related to the evacuation. Escort guards are furnished by the command (division and above) to which the detainees are being evacuated.

STEP 6. TAG

D-16. When the detainees have been searched and segregated, the capturing unit prepares a capture tag and puts one on each detainee. It is very important that the capturing unit fill out the Capture Tag as accurately and completely as possible. HUMINT collectors will use the information from the tag when preparing to interrogate detainees. The "capturing unit" and "location of capture" information will be used to provide direct feedback to the capturing unit when information of immediate tactical value is obtained. Each EPW tag has a different serial number used for the purpose of accountability and cannot be reproduced. The EPW tag is perforated into three parts: Part A is attached to the detainee, Part B is retained by the capturing unit, and Part C is attached to the detainee's property (see Figure D-1).

DOCUMENT HANDLING

DOCUMENTS FOUND ON ENEMY PRISONER OF WAR

D-17. The battalion S2 and subordinate unit commander ensure that CEDs found on detainees are handled as follows. The capturing unit will—

- Search each detainee.
- Return identification documents to detainees. It may be preferable to return only one identity document, to preclude the detainee from spreading extras around to cause confusion. The preferred ID document to return to the detainee is a picture ID (such as a military

or government ID card). If the detainee has several identification documents, the S2 returns the ID that most accurately reflects the detainee's official status. This might be a military ID for a soldier and a passport or government-issue ID for a civilian. If the detainee has several identification documents with different names, this may be an indicator of CI interest. The S2 notifies the nearest CI unit.

- Write the following on the top and bottom half of the EPW capture tag: Number of documents taken, date and time, location and circumstances of capture, capturing unit's designation.
- Put CEDs in a waterproof bag, one per detainee.
- Affix Part C of the capture tag to the bag.
- Give CEDs to the senior escort.
- Direct the senior escort to evacuate CEDs with the detainee.

DOCUMENTS FOUND IN THE AO

D-18. An example of CEDs found in the AO is paperwork discovered in an overrun CP, but not on a detainee. The capturing unit will—

- Put CEDs in a waterproof bag.
- Follow the same procedures described above, and tag the bag.
- Evacuate the CEDs to the battalion S2.
- Evacuate all CEDs as dictated by Annex B of the OPORD. This is normally through the MI chain (for example, from Battalion S2 to Brigade S2, to the first HUMINT collection or DOCEX unit in the MI chain). The S2 normally coordinates with the S4 for the use of supply vehicles returning empty to the rear for the transportation of large numbers of documents.

INITIAL DOCUMENT EXPLOITATION

D-19. A combat unit without language-qualified personnel can perform limited battlefield DOCEX, mainly on maps and overlays. The unit S2 is normally responsible for any initial exploitation by the capturing unit. The S2 safeguards the items pending disposition. At the same time he—

- Looks over the document.
- Does not mark or harm it in anyway.
- Uses whatever resources are available to decipher it; for example, dictionaries and enemy map symbol guides.
- Looks for information that has a direct bearing on his current mission.

D-20. The S2 extracts the combat information and uses the SALUTE format as a template to organize the information.

EQUIPMENT HANDLING PROCEDURES

D-21. CEE includes all types of foreign materiel found on a detainee or in the AO that may have military application. The capturing unit—

- Always permits the detainee to keep protective equipment and equipment for his personal well being unless this gear is replaced by equivalent items by the capturing unit. This equipment includes helmet, NBC gear, mess gear (excluding knife and fork).
- Disposes of equipment in accordance with unit SOPs and instructions in Annex B of the OPORD. Most routine equipment is normally destroyed in place. Unusual or new equipment or equipment identified as being of TECHINT interest is tagged with a CEE tag (Part C of DD Form 2745) and evacuated to the nearest TECHINT unit. Communications equipment is also tagged and evacuated to the nearest SIGINT unit.
- Identifies equipment that cannot be easily evacuated; its location is passed through intelligence channels to the nearest unit that will be involved in its exploitation.

FIELD-EXPEDIENT TAGGING PROCEDURES

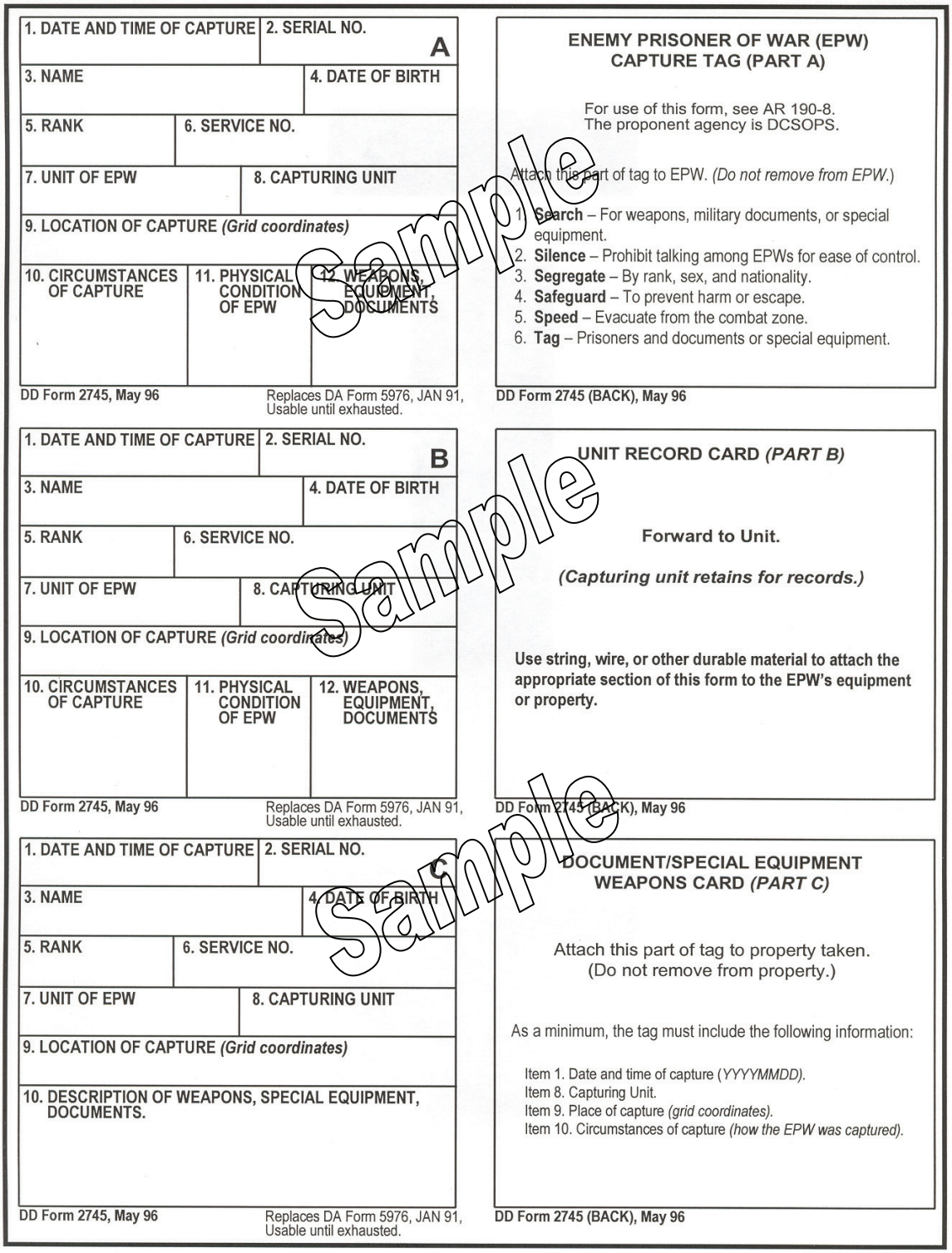
D-22. When no standard tag forms are available, the following field-expedient methods may be used:

- Use meals, ready-to-eat (MRE) cardboard or other type of paper.
- Write the capturing unit's designation.
- Write data and time of capture.
- Write POC coordinates.
- Write circumstances of capture.
- Identify EPW, captured document, or equipment captured.
- Put tag, without damaging the CED, in a waterproof bag.
- Attach EPW and CEE tags so they will not come off.

MEDICAL CARE

D-23. Medical equipment and supplies to permit the administering of emergency first aid should be available at each EPW collecting point and EPW holding area. A qualified medical retained person, if available, may administer first aid to other detainees. All detainees suspected of having communicable diseases are isolated for examination by a medical officer. Wounded detainees may be questioned by intelligence personnel once the detainees are cleared by competent medical authority for questioning.

D-24. For evacuation purposes, detainees may be classified as walking wounded or sick, or as non-walking wounded or sick. Walking wounded detainees are evacuated through MP EPW evacuation channels. Non-walking wounded are delivered to the nearest medical aid station and evacuated through medical channels.



1. DATE AND TIME OF CAPTURE | 2. SERIAL NO. A
3. NAME | 4. DATE OF BIRTH
5. RANK | 6. SERVICE NO.
7. UNIT OF EPW | 8. CAPTURING UNIT
9. LOCATION OF CAPTURE *(Grid coordinates)*
10. CIRCUMSTANCES OF CAPTURE | 11. PHYSICAL CONDITION OF EPW | 12. WEAPONS, EQUIPMENT, DOCUMENTS

DD Form 2745, May 96 — Replaces DA Form 5976, JAN 91, Usable until exhausted.

ENEMY PRISONER OF WAR (EPW) CAPTURE TAG (PART A)

For use of this form, see AR 190-8.
The proponent agency is DCSOPS.

Attach this part of tag to EPW. *(Do not remove from EPW.)*

1. **Search** – For weapons, military documents, or special equipment.
2. **Silence** – Prohibit talking among EPWs for ease of control.
3. **Segregate** – By rank, sex, and nationality.
4. **Safeguard** – To prevent harm or escape.
5. **Speed** – Evacuate from the combat zone.
6. **Tag** – Prisoners and documents or special equipment.

DD Form 2745 (BACK), May 96

1. DATE AND TIME OF CAPTURE | 2. SERIAL NO. B
3. NAME | 4. DATE OF BIRTH
5. RANK | 6. SERVICE NO.
7. UNIT OF EPW | 8. CAPTURING UNIT
9. LOCATION OF CAPTURE *(Grid coordinates)*
10. CIRCUMSTANCES OF CAPTURE | 11. PHYSICAL CONDITION OF EPW | 12. WEAPONS, EQUIPMENT, DOCUMENTS

DD Form 2745, May 96 — Replaces DA Form 5976, JAN 91, Usable until exhausted.

UNIT RECORD CARD *(PART B)*

Forward to Unit.

(Capturing unit retains for records.)

Use string, wire, or other durable material to attach the appropriate section of this form to the EPW's equipment or property.

DD Form 2745 (BACK), May 96

1. DATE AND TIME OF CAPTURE | 2. SERIAL NO. C
3. NAME | 4. DATE OF BIRTH
5. RANK | 6. SERVICE NO.
7. UNIT OF EPW | 8. CAPTURING UNIT
9. LOCATION OF CAPTURE *(Grid coordinates)*
10. DESCRIPTION OF WEAPONS, SPECIAL EQUIPMENT, DOCUMENTS.

DD Form 2745, May 96 — Replaces DA Form 5976, JAN 91, Usable until exhausted.

DOCUMENT/SPECIAL EQUIPMENT WEAPONS CARD *(PART C)*

Attach this part of tag to property taken.
(Do not remove from property.)

As a minimum, the tag must include the following information:

Item 1. Date and time of capture (*YYYYMMDD*).
Item 8. Capturing Unit.
Item 9. Place of capture *(grid coordinates)*.
Item 10. Circumstances of capture *(how the EPW was captured)*.

DD Form 2745 (BACK), May 96

Sample
Sample
Sample

Figure D-1. DD Form 2745 (Enemy Prisoner of War Capture Tag).

This page intentionally left blank.

Appendix E

Extracts from Allied Joint Publication (AJP)-2.5

Following are excerpts from Allied Joint Publication-2.5, Handling of Captured Personnel, Equipment and Documents. AJP-2.5 is primarily an amalgamation of procedures outlined in STANAG 2033, STANAG 2044, and STANAG 2084, and will be used as the authoritative source for matters governed by those STANAGs. S2s and HUMINT collectors should maintain a copy on hand.

THE GENEVA CONVENTIONS

E-1. Treatment of prisoners of war (PWs) and other detainees as well as the handling of personal possessions including personal documents belonging to them will at all times be in accordance with the 1949 Geneva Conventions and, if ratified by the nations concerned, with the 1977 Protocols.

THE DETAINING POWER

E-2. The responsibilities of the "Detaining Power" as set out in GC3 shall rest with the nation or the deployed NATO command which initiated the capture or detention of the person or persons in question.

E-3. Transfers of PWs between NATO nations must be in accordance with GC3, Article 12, as interpreted but not superseded by national agreements.

KNOWLEDGE OF THE GENEVA CONVENTIONS AND THE 1977 PROTOCOLS

E-4. The Geneva Conventions require the signatories in time of both peace and war to circulate the text of the Conventions as widely as possible within their countries. They are especially required to ensure that the provisions and implications of the Conventions are clearly understood by the members of their armed forces and by the civilians attached to them. In order to assist this process, it is suggested in the Conventions that instruction in them is included in the syllabus of appropriate military and civilian courses of instruction.

E-5. The conventions also state that any military or other authority assuming responsibility for dealing with PWs in time of war or armed conflict must be in possession of the text of the Conventions and that its personnel must be instructed in how the Conventions affect them in the execution of their duties with PWs.

E-6. If ratified by the nations concerned, these requirements are, by inference, also applicable to the 1977 Protocols.

PRISONER-OF-WAR STATUS

E-7. Captured personnel (CPERS) can be divided into two categories: Captured personnel who are PWs and other detainees.

E-8. Prisoner-of-war status is conferred on captured personnel who fall within the categories listed in Article 4 of GC3, which is reproduced in Annex A, or, if ratified by the nations concerned, those who meet the expanded definition of a PW as stated in Protocol I of the 1977 Protocols.

E-9. Other detainees are personnel being held by NATO forces until their status can be determined and their further disposition can be decided.

E-10. Furthermore, when NATO forces are engaged in Peacetime Support Operations (PSOs), the operational plan should contain specific instructions as to which individuals will have PW status. Directions for handling other detainees, including those suspected of crimes against humanity and war crimes, are also to be included in the operational plan or in the Standing Operating Procedures used in the operation.

PERSONNEL

E-11. Conditions allowing, the following procedures should be followed by the capturing unit:

a. CPERS should be disarmed immediately, and all documents and effects of military or investigative interest except for necessary clothing, identity documents and protective equipment (Geneva Convention Relative to the Treatment of Prisoners of War (GC3), Article 18) should be removed. CPERS should then be tagged in accordance with the procedures outlined at Annex B. A Common Capture Report should also be completed and forwarded in accordance with the procedure set out in Annex C. It is important that the documents, equipment, maps, etc., taken from a CPERS accompany him to the next receiving unit. Valuable information may be lost by not having these items available during processing and interrogation.

b. Within the confines of the tactical situation, CPERS are to be segregated according to rank, grade, service, sex and nationality or ethnic group/warring faction to minimize the opportunity to prepare counter-interrogation measures. Furthermore, deserters, civilians and political indoctrination personnel will be individually segregated from other CPERS. Such segregation shall be undertaken in a manner which does not violate GC3, Article 16.

c. Talking or fraternization between CPERS is to be prevented in order not to prejudice future intelligence collection operations. CPERS will be allowed no opportunity to exchange information between themselves, to exchange identities or to dispose of articles of intelligence interest.

d. Interrogation operations must not be compromised by contact between CPERS and personnel not concerned with interrogation duties.

e. CPERS will also be prevented from observing sensitive and critical activities, equipment and procedures involving NATO, national or allied forces.

f. CPERS are to be guarded in a manner which shall deny them the opportunity for escape or sabotage.

g. Defectors and political refugees should also be segregated from other CPERS wherever possible. These personnel shall be screened by the nearest Interrogation Unit (IU), which will decide on their value to the intelligence organization and consequent future movements. In all cases, defectors are to be treated in accordance with the Geneva Convention Relative to the Protection of Civilians in Time of War (GC4). National policy may provide defectors treatment in accordance with GC3 where such treatment provides greater protection than GC4.

h. Personnel claiming to be agents of an allied power shall also be segregated from other CPERS. The intelligence organization (G2 or CJ2) is to be informed of all such individuals as soon as possible and will arrange for their screening to determine their future disposition.

i. CPERS suspected of crimes against humanity and war crimes will also be segregated from other prisoners. Legal authorities and the intelligence organization are to be informed of such suspects as soon as possible. They will be taken into custody by law enforcement personnel. Intelligence exploitation should be undertaken in cooperation with the legal authorities.

j. All CPERS are to be treated humanely.

k. Naval and Air Force personnel are to be identified and the intelligence organization is to be notified in order that interrogation by naval/air force personnel may take place at the earliest opportunity.

l. CPERS are to be escorted to the nearest Collecting Point or Holding Area as quickly as possible.

m. Should any doubt arise as to whether any persons, including those appearing to be PWs, having committed a belligerent act and having fallen into Allied hands, belong to any of the categories of persons entitled to PW status pursuant to Article 4 of GC3, such persons shall enjoy the protection of GC3 until such time as their status has been determined by a competent tribunal. If such a tribunal determines that an individual does not qualify for PW status, then the detaining commander must determine whether the detainee qualifies as a ”protected person” pursuant to GC4, and obtain legal advice relative to the proper course of action for dealing with such detainees.

DOCUMENTS

E-12. Captured documents (CDOC) considered of intelligence interest will be handled by the capturing unit in the following manner:

a. The capturing unit will conduct a preliminary screening to obtain information of immediate technical or tactical value.

b. An intelligence report (INTREP) identifying the CDOC and its disposition as well as giving information considered to be of immediate tactical value will be prepared and submitted by the capturing unit. (See STANAG 2022.)

c. The capturing unit will tag or otherwise mark the CDOC as follows:

- National identifying letters of capturing unit as prescribed in STANAG 1059.
- Designation of capturing unit including service.
- Serial number of the CDOC. This will consist of a number allocated sequentially by the capturing unit.
- DTG of capture.
- Location of capture (geographic coordinates or UTM grid reference including grid zone designation and 100,000-meter square identification).
- Captured from Unit (enemy or warring faction) (including national identifying letters in accordance with STANAG 1059).
- Summary of circumstances under which the CDOC was obtained. Interrogation serial number of any associated CPERS, if appropriate or known.
- CED associated with a captured person should be marked with part C of the Standardized EPW Capture and Personal Equipment Tag.

d. CED to be used as evidence in legal proceedings against CPERS suspected of crimes against humanity and war crimes will be kept under guard or in a secure area separate from other CED.

EQUIPMENT

E-13. Captured Equipment (CE) and Associated Technical Documents (ATDs) considered of intelligence interest will be handled by the capturing unit in the following manner:

a. A Capture Report as set out in Annex C of the OPORD will be prepared by the capturing unit upon the discovery or capture of CE or ATD believed to be of intelligence interest. The reporting channels are from the capturing unit through the chain of command to the first TECHINT element.

b. The capturing unit will conduct a preliminary screening to obtain information of immediate technical or tactical value. A Preliminary Technical Report (PRETECHREP) as set out in Annex D of the OPORD will be prepared and submitted through established intelligence channels.

c. Intelligence Reports (INTREP) may, as circumstances dictate, be submitted in advance but not in lieu of the Capture Report and PRETECHREP. (See STANAG 2022.)

d. CE and ATD will be tagged or marked by the capturing unit as follows:

- National identifying letters of capturing unit as prescribed in STANAG 1059.
- Designation of capturing unit including service.
- DTG of capture.
- Location of capture (geographic coordinates or UTM grid reference including grid zone designation and 100,000-meter square identification).

- Captured from Unit (enemy or warring faction) (including national identifying letters in accordance with STANAG 1059).
- Summary of circumstances of capture.
- Associated CPERS.

e. CE and ATD to be used as evidence in legal proceedings against CPERS suspected of crimes against humanity and war crimes will be kept under guard separate from other CE and ATD.

This page intentionally left blank.

Appendix F

NATO System of Allocating Interrogation Serial Numbers

1. Every captured person selected for interrogation will be given an Interrogation Serial Number. This number shall be allocated by the Interrogation Unit conducting the **first** interrogation of the captured person.

2. The number should not be confused with the Prisoner of War Internment Serial Number (ISN), which is to be used for administrative purposes only.

3. The purpose of the Interrogation Serial Number is to identify the source of information to ensure its proper evaluation, processing, and follow-up action. It will also identify the nationality and location of the interrogation unit.

4. The number shall be constituted as follows:

a. 2 letters to indicate the Nationality of the captured person (see para 6).

b. 2 letters to indicate the Service of the captured person (see para 7).

c. 1 letter to indicate the Arm of Service of the captured person (see para 8).

d. 4 numbers to indicate the Interrogation Sequence Number of the captured person (see para 9).

e. 4 numbers to indicate the Day and Month of Capture.

f. A dash (-) to show a sequence break.

g. 4 letters to indicate the Nationality and Service of the Interrogation Unit (see para 10).

h. 4 letters to indicate the Interrogation Unit.

5. Each group shall be separated by a dash. The final number shall therefore appear as in the following examples:

LS – NV – B – 0012 – 2105 – USNV – 0159

Liechtenstein – Naval prisoner – Seaman – 12th captured person interrogated - captured 21 May – interrogated by US Navy – team 159

AN – AF – H – 0357 – 0211 – GEAF – 0007

Andorra – Air force prisoner – Intelligence – 357th captured person interrogated – captured 2 Nov – interrogated by GE Air Force – team 7

SM – AR – X – 0431 – 0707 – UKAR – 0019

San Marino – Army prisoner – One star or above – 431st captured person interrogated – captured 7 Jul – interrogated by UK Army – team 19

6. The two letters used for indicating the Nationality of the captured person will be in accordance with established NATO Country codes in STANAG 1059.

7. The following list of letters is to be used to indicate the Service of the captured person:

AR	- Army	NI	- Naval Infantry
NV	- Navy	AB	- Airborne Forces
NA	- Naval Air Arm	SF	- Special Purpose Forces
AF	- Air Force	PL	- Police
IR	- Irregular	CV	- Civilian (other than Police)

8. The following list of letters is to be used to indicate the Arm of Service of the captured person:

Navy (A)	**Army (B)**	**Air Force (C)**	**Other/Partisan Forces (D)**
A. Aircrew	Aircrew	Aircrew	Aircrew
B. Seamen	Infantry	Ground Crew	Merchant Marine
C. Communications	Signals	Communications	Radio Officers/Operators
D. Weapons/ Electronic Engineer	Electrical/Electronic Engineer	Electrical/Electronic Engineer	
E. Mechanical/ Marine/Engineers	Engineers	Mechanical/Air Frame/Engineers	
F. Gunnery	Artillery	Ordnance	Weapons/Ordnance Explosives
G. *HQ Staff	*HQ Staff	*HQ Staff	*HQ Staff
H. Intelligence	Intelligence	Intelligence	Intelligence
I. Marines	Airborne Forces	Airfield Defense	
J. Cooks/Stewards	Catering	Catering	Catering
K. Legal/Political	Legal/Political	Legal/Political	Legal/Political
L. Medical/Dental/ Nursing	Medical/Dental/ Nursing	Medical/Dental/ Nursing	Medical/Dental/ Nursing
M. Electronic Warfare	Electronic Warfare	Electronic Warfare	Electronic Warfare
N. Operations	Operations	Operations	Operations
O. Police	Police	Police	Police
P. Supply	Quartermaster	Supply	Supply
Q. Strategic Weapons	Strategic Weapons	Strategic Weapons	Strategic Weapons
R. Special Purpose Forces	Special Purpose Forces	Special Purpose Forces	Special Purpose Forces
S. Air Traffic Control	Armored	Air Traffic Control	Air Traffic Control
T. *Unknown	*Unknown	*Unknown	*Unknown

Navy (A)	Army (B)	Air Force (C)	Other/Partisan Forces (D)
U. Instructors	Education	Education	Instructors
V. Ministers of Religion	Ministers of Religion	Ministers of Religion	Ministers of Religion
W. *Submarines	Artillery Spotters	Forward Air Controllers	Couriers, etc.
X. *One Star +	*One Star +	*One Star +	*Officers in Command of Irregular Forces
Y. *Other	*Other	*Other	*Other
*Notes: G – Headquarters staffs below one star rank T – Captured Person's arm of service not known to report writer W – To be used in respect of all submarines regardless of arm or specialization X – To be used in respect of all ONE STAR or above officers regardless of army Y – PW arm of service not included in the appropriate list			

9. The sequence number of the interrogated captured personnel shall be of four digits allocated in numerical order of interrogation by the team first interrogating the captured person.

10. Country, services and team codes.

a. Country codes, as laid down in STANAG 1059, are to be used for indication of the Nationality of the Interrogation Team.

b. The following lists of letters are to be used for indicating the Service of the Interrogation Team:

ARMY	- AR	AIR FORCE	- AF
NAVY	- NV	MARINE	- MR
COAST GUARD	- CG	PARA-MILITARY	- PM

c. NATO teams will use the following abbreviations: (These will be determined as command changes are implemented and STANAG 1059 is revised).

SC EUROPE	RC SOUTH
RC NORTH	JHQ SOUTHWEST
JHQ NORTH	JHQ SOUTH
JHQ NORTHEAST	JHQ SOUTH CENTER
JHQ CENTER	JHQ SOUTHEAST
CC AIR NORTH	CC AIR SOUTH
CC NAV NORTH	CC NAV SOUTH
SC ATLANTIC	RC EAST
RC WEST	STRIK FLTLANT
RC SOUTHEAST	SUB ACLANT

11. Nations will allocate 4-digit serial numbers to their interrogation teams. NATO Commands will issue similar numbers to subordinate national interrogation teams under their command.

This page intentionally left blank.

Appendix G

Questioning Quick Reference

This appendix offers a quick reference for the trained HUMINT collector. It is not meant to be all-inclusive, nor instructive in proper questioning technique, but lays out frequently used requirements grouped logically by OB factor. Proper formation of questions is covered in detail in Chapter 9.

Missions: Mission questioning consists of three areas: Time of Capture Mission, Future Mission, and Past Mission. Missions are questioned in that order, to ensure that the information is collected in the order of importance to a supported commander. Logical follow-up questioning may lead the collector into any of the OB factors at any time during questioning in order to provide complete information.

Offensive Missions:
When will the enemy attack?
Where will they attack?
What is the main objective of the attack?
What units will participate in the attack?
What tactics will be employed?
What artillery, air, and other units will support the attack?

Defensive Missions:
Where will the enemy establish lines of defense?
What units have been assigned to the defensive lines?
What obstacles have been emplaced (mines, trenches, wire, etc.)?
What artillery support is there for the defensive operation?

Retrograde Operations:
What units will take part in the retreat?
What are the current positions of the retreating units?
When will they start to retreat?
What routes will be used?
What is the planned destination of the retreating units?
What units will cover the retreat?

Composition:
What is the command and control element of (the target unit)?
What types of units are directly subordinate to (the target unit)?
What is the designation of (each of the subordinate units)?
How many units of that type are directly subordinate to (target unit)?
What units are attached? When? Why? What unit(s) are they detached from?
What units are detached? When? Why? What unit(s) are they attached to now?

Weapons and Equipment Strength:

Individual Weapons:
What individual weapons are there in (target unit)?
How many?
What is the distribution of the weapons?
Crew-Served Weapons: What crew-served weapons are in (target unit)?
How many?
What is the distribution of the weapons?
Other Weapons: What other weapons are there in (target unit)?
What types?
How many?
How are they distributed?
Vehicles: What armored vehicles are in (unit)?
How many?
What nomenclature?
What other vehicles are in (unit)?

Dispositions:

Disposition questioning is ideally done with the aid of a map.
Where is (the target disposition)?
Show (on the map) the location of (the target disposition).
What enemy units, activities, or equipment are at that location?
What security measures are being employed at that location?
Additionally, specific types of dispositions require additional follow-up:

Area-Type Dispositions: (Staging Areas, Assembly Areas, Trains, etc.)
Show on the map (or describe) the perimeter of the disposition.
Where are units or activities located within it?
Where are the approaches/entrance?
What unit is in charge?
What vehicles or equipment are located within the disposition?
What is the date of information?

Line-Type Dispositions: (Line of Departure, Artillery emplacement, etc.)
Show on the map (or describe) the location of the disposition.
Define and locate both ends of the disposition.
What equipment is located there?
In the case of artillery, describe the placement and orientation of the guns, ammunition, radar, and support vehicles.

Tactics:

Offensive: What offensive tactics are being employed by (unit)?
What other units are involved?
When did (unit) begin employing these tactics?
What are the major objectives?
Defensive: What defensive tactics are being employed by (unit)?
What other units are involved?
When did (unit) begin employing these tactics?
Special Operations: What special operations tactics are being employed by (unit)?
What are the designations of the units employing special operations tactics? When did (unit) begin employing special operations tactics?
Where/Why are these tactics being employed?

Training:

Individual Training: What individual training is being conducted by (unit)?
Who is being trained?
How effective is the training?
Where is the training conducted?
What are the training standards?
Unit Training: What unit training is being conducted by (unit)?
Who is being trained?
How effective is the training?
Where is the training conducted?
What are the training standards?
Specialized Training: What specialized training is being conducted by (unit)?
Who is being trained?
How effective is the training?
Where is the training conducted?
What are the training standards?
What specialized equipment is used in the conduct of the training?

Combat Effectiveness:

Losses:
Personnel: What personnel losses have been incurred by (unit)?
When? Where? How?
What were the duty positions/ranks of the lost personnel?
Equipment: What equipment losses have been sustained by (unit)?
What type of equipment was lost?
When? Where? How many?
How were they lost?

Replacements (Personnel):

Received: What replacements have been received by (unit)?
What replacements are available to (unit)?
How many?
From where were the replacements received?
Available: What personnel replacements are available to (unit)?
From where are replacements available?
How many? What ranks?
How long would it take for replacements to arrive once requested?

Replacements (Equipment):

Received: What equipment replacements have been received by (unit)?
How many?
From where were the replacements received?
How does the quality of the replacement equipment compare to that of the original equipment?
What is the level of confidence in the replacement equipment, compared to the original?
Available: What equipment replacements are available to (unit)?
From where are replacements available?
How long would it take to receive replacement equipment once requested?
How many of each type of equipment are available?

Reinforcements:

Received: What reinforcements have been received by (unit)?
What type was the reinforcing unit?
What is the designation of the reinforcing unit?
What equipment did the reinforcing unit bring?
To which unit was the reinforcing unit further assigned?
Why did (receiving unit) receive reinforcements?
How long will the reinforcing unit be assigned as reinforcement to (unit)?
Available: What reinforcements are available to (unit)?
From where (parent unit/location) are reinforcements available?
What types of units are available to reinforce (unit)?
How long would it take for reinforcements to arrive, once requested?

Morale:

Describe the morale of the members of (unit).
How long has the morale been…?
What is the unit leadership doing to (maintain/improve) the morale?
What effect has (high/low) morale had on the behavior or performance of the unit members?

Logistics:

Weapons: What is the condition of the (specific weapons) in (the unit)?
Why are (the weapons) in that condition?
What is being done to improve the condition of (the weapons)?
How often is maintenance performed? By whom?
Who inspects weapons? How often?
Is there an increased emphasis on maintenance? If so, why?
What is done to prevent/alleviate a shortage while weapons are being maintained?
What spare parts are there for weapons in (unit)?
What shortages of spare parts are there?
What problems are there with spare parts (quality, fit, delays, etc)?
Ammunition: What types of ammunition are available for the (weapon/weapon system) in the (unit)?
What problems are being experienced with ammunition for (weapon or weapon system) in (unit)? Why? Since when?
What is being done to correct the problem(s)?
What shortages of ammunition for (weapon or weapon system) are there in (unit)?
What is being done to correct the shortage?
When was the last issue of ammunition for the (weapon or weapon system) in the (unit)?
How much was issued?
When is the next issue of ammunition planned?
(For insurgents/irregulars - Where is funding obtained for ammunition/explosive purchases?
Where are ammunition/explosives obtained?
How are ammunition/explosives transported/delivered?
Vehicles: What is the condition of the (specific vehicle) in (the unit)?
Why are (the vehicles) in that condition?
What is being done to improve the condition of (the vehicles)?
How often is maintenance performed? By whom?
Who inspects vehicles? How often?

Is there an increased emphasis on maintenance? If so, why?
What is done to prevent/alleviate a shortage while vehicles are being maintained?
What spare parts are there for vehicles in (unit)?
What shortages of spare parts are there?
What problems are there with spare parts (quality, fit, delays, etc)?

POL:

What problems have been experienced with the petroleum, oils, and lubricants (POL) for the (vehicle type) in the (unit)?
Why are there problems?
Since when have there been problems?
What is being done to correct the problems?
What shortages of POL are there? Why?
What is being done to alleviate the shortages?
When was the last resupply of POL in (unit)? Where? How much?
When is the next resupply of POL planned?

Communications Equipment:

What is the condition of the (specific radio set) in (the unit)?
Why are (the radios) in that condition?
What is being done to improve the condition of (the radios)?
How often is maintenance performed? By whom?
Who inspects communication equipment? How often?
Is there an increased emphasis on maintenance? If so, why?
What is done to prevent/alleviate a shortage while radios are being maintained? What spare parts are there for communication equipment in (unit)?
What shortages of spare parts are there?
What problems are there with spare parts (quality, fit, delays, etc)?

Medical:

Equipment: What individual medical equipment is in (unit)? How many?
What is the distribution?
What are the contents of individual medical kits in the (unit)?
What is the quality?
What shortages are there?
What problems are there with the individual medical equipment/supplies in (unit)?
What vehicular medical equipment is in (unit)? How many?
What is the distribution?
What are the contents of vehicular medical kits in (unit)?
What is the quality?
What shortages are there?
What problems are there with the vehicular medical equipment/supplies in (unit)?

Personnel: What medical personnel are assigned to (unit)?
What medical personnel are available to treat members of (unit)? How many? What are the duty positions of the medical personnel?
What level of medical care are the medical personnel able to provide to members of (unit)?

Facilities: What medical facilities are available to members of (unit)?
Where are the medical facilities?
What level of care is available there?
What higher echelons of medical care are available?

Medical Evacuation (MEDEVAC) Procedures: What MEDEVAC procedures are available to members of (unit)?
Where are MEDEVAC collection points?
What different MEDEVAC procedures are used for more seriously wounded personnel, compared to lightly wounded?
Food: What rations are members of (unit) eating?
What shortages are there of food?
What is the quality?
What problems have been encountered with the rations provided to (unit)?
When was the last issue of rations to members of (unit)?
When is the next issue?
What reserve stocks of field rations are there in (unit)?
Water: What is the source of drinking water for members of (unit)?
What problems have been encountered with quality, shortages, or contamination of drinking water?
What water purification methods are available to members of (unit)?
Under what circumstances will they be used?
If water purification tablets are used, what color are they?

Electronic Technical Data:

Radio Frequencies: What are the primary and alternate frequencies for radios in (each unit)?
Under what circumstances will alternate frequencies be used?
What networks operate on the various frequencies?
Call Signs: What is the call sign of (unit)?
What is the call sign of (each) person of authority in the unit?
When do call signs change?
What informal call signs are in use?

Miscellaneous:

Personalities: Question for name, rank, unit, duty position, and unit of key leaders.
Collect identifying characteristics such as age, height, weight, build, hair and eye color, writing hand, facial hair and teeth.
Report contact information such as work and home addresses, telephone numbers, fax number, and email address.
Complete biographical IIR format is in DIAM 58-12 (S//NF).
Code Names: What is the code name of (each unit)?
What code names are being used for specific operations?
Passwords: What is the current challenge/password for (unit)?
When did it go into effect?
When will it change?
What will the next challenge/password be?
What other (informal, "run in") passwords are in use?

Obstacles:

Enemy: What obstacles have the enemy forces emplaced?
Where, when, what type of obstacles?
What safe lanes are there through or around the obstacles?
(If mine fields, collect type, pattern, quantity, and method of emplacement of mines.)
How are the obstacles being covered (artillery, ambush, etc.)?

Why have the obstacles been emplaced where they are (denial of terrain, canalization into a fire sack, etc.)?

Friendly: What friendly obstacles have enemy forces encountered? Where? When?

Have those obstacles been breached or otherwise neutralized?

What effect have the friendly obstacles had on enemy maneuver?

PSYOP:

Enemy: What PSYOP are being conducted by (unit)?

What is the text of the messages?

Who is the target audience?

Where are the PSYOP materials prepared?

Where and how are they delivered? What is the hoped-for effect?

Friendly: What PSYOP have members of (unit) encountered? Where? When?

What form of PSYOP was encountered?

What effect have the PSYOP had on the officers/NCOs/enlisted of (unit)?

What is the leadership of (unit) doing to counter the effects of friendly PSYOP?

This page intentionally left blank.

Appendix H

SALUTE Reporting

H-1. The SALUTE report format requires brief entries which require the collector to break information down into basic elements: who, what, where, when, why, and how. This allows for efficient reporting via electronic or hardcopy medium. It also allows the analyst to quickly scan multiple reports to find specific information.

H-2. Figure H-1 provides guidance and is not to be construed as strict requirements. SALUTE reports of combat activity may only contain a word or two in each entry, whereas Intelligence reports tend to include more detail.

TO: Usually the address of the supported S2/G2 (according to unit SOP)

FROM: Your unit or team designation, or your duty position, as appropriate

DTG: The date-time group of when the report is being submitted

Report Number: From local SOP

1. (S)ize/Who: Expressed as a quantity, and echelon, or size (e.g., 1 x BDE). If multiple echelons are involved in the activity being reported, there can be multiple entries (e.g.,1 x BDE; 2 x BN). Non-standard units are reported as such (e.g., bomb-making class; support staff).

2. (A)ctivity/What: This line is the focal point of the report and relates to the PIR or important non-PIR information being reported. It should be a concise bullet statement.

3. (L)ocation/Where: Generally a grid coordinate, including the 100,000 meter grid zone designator. The entry can also be an address, if appropriate, but still should include an 8-digit grid coordinate. City names will always be followed by the two-character country code. If the activity being reported involves movement (advance, withdrawal, etc.) the location entry will include "From" and "To" entries. The route used will be reported under "Equipment/How."

4. (U)nit/Who: This entry identifies who is performing the activity described in the "Activity/What" entry. Include the complete designation of a military unit, identification of a civilian or insurgent group, or the full name of an individual, as appropriate.

5. (T)ime/When: For a future event, this is when the activity will initiate. Past events are usually not the subject of SALUTE reports, but if a past event is to be reported, the Time/When entry will generally reflect when the event ended. Ongoing events are reported as such. Reports of composition of forces, morale, and Electronic Technical Data and other non-event topics are reported as ongoing. When reporting on a disposition, the "Time/When" entry is generally the last time the source was at the disposition.

6. (E)quipment/How: The information reported in this entry clarifies, completes, and/or expands upon information reported in any of the previous entries. It includes information concerning equipment involved, tactics used, and any essential elements of information not reported in the previous paragraphs.

7. Remarks: Use this entry to report the source of the information, whether a person, a CED, open-source media, or other source. Include the date of information and the PIR that the reported information addresses. Map data for coordinates given in the "Location/Where" entry are included, stating map series name, sheet number, scale and edition. If there are enclosures to the SALUTE report, such as sketches, they are annotated here.

Figure H-1. Example of a Written SALUTE Report.

Appendix I

Document Exploitation and Handling

I-1. DOCEX is a vital information source in the development of the all-source intelligence picture. Unless planned for and carefully monitored, the volume of CEDs in all operations can rapidly overwhelm a unit's capability to extract meaningful information.

DEFINITIONS

I-2. A document, as defined by AJP 2.5, is any piece of recorded information, regardless of form. Documents include printed material such as books, newspapers, pamphlets, OPORDs, and identity cards as well as handwritten materials such as letters, diaries, and notes. Documents also include electronically recorded media such as computer files, tape recordings, and video recordings and the electronic equipment which contains documents or other vitally important intelligence. Examples include hard drives, operating systems, and personal electronic devices, including phones, PDAs, and GPS devices. A CED may be needed by several collection or exploitation activities at the same time, requiring copies to be made. Collectors must have ready access to copying equipment. Documents often must be evacuated through two different channels for proper exploitation, which also makes copying necessary. Such documents and equipment require special handling to assure that they are returned to their owners.

I-3. DOCEX is the systematic extraction of information from threat documents for the purpose of producing intelligence or answering IRs. A threat document has been in the possession of the threat, written by the threat, or is directly related to a future threat situation. DOCEX can occur in conjunction with HUMINT collection activities or as a separate activity.

I-4. A CED is any document that was in the possession of an enemy force that subsequently comes into the hands of a friendly force, regardless of the origin of that document. There are three types of CEDs.

- Official - documents of government or military origin.
- Identity - personal items such as identification (ID) cards or books, passports, driver licenses.
- Personal - documents of a private nature such as diaries, letters, and photographs.

I-5. Open-source documents are documents that are available to the general public including but not limited to newspapers, books, videotapes, public records, and documents available on the Internet or other publicly available electronic media.

I-6. Source-associated documents are documents that are encountered on or in immediate association with a human source. These may include both official and personal documents. Documents associated with human sources are normally exploited, at least initially, during the interrogation or debriefing of the source. Interrogators typically use these documents during planning and preparation for interrogation of the associated EPW. These personal documents and source identification documents are therefore evacuated in conjunction with the associated source and sent through prisoner, detainee, or refugee evacuation channels rather than through intelligence channels. If the duplication capability exists, collectors should copy personal documents that contain intelligence information and evacuate the copy through intelligence channels. The original personal document should be evacuated with the detainee but not on his person until the HUMINT collector has exploited it. Collectors evacuate official documents through intelligence channels after initial exploitation. If possible, the collector will copy official documents and evacuate the copy with, but not on, the source.

OPEN-SOURCE INFORMATION

I-7. Open-source information is publicly available information appearing in print or electronic form. Open-source information may be transmitted via radio, television, newspapers, commercial databases, electronic mail networks, or other electronic media like CD-ROMs. Whatever form they take, open sources are not—

- Classified at their origin.
- Subject to proprietary constraints.
- The product of sensitive contacts with US or foreign persons.

I-8. In all operations, open-source collection can be a valuable addition to the overall intelligence collection and each intelligence discipline's efforts. Open-source information supplements the HUMINT collection effort, and all types of open sources must be considered for exploitation.

I-9. Open sources are evaluated and categorized as friendly, neutral, or hostile. Certain high-value, open-source information sources may be identified for continuous monitoring. Other open-source information sources may be identified to screen for the presence or lack of specific indicators. In addition, the information obtained from open sources is extremely helpful for the HCT members to be current with the latest developments in the AO, which enables them to establish rapport and effectively converse with their sources. Open-source documents are exploited in the same manner as CEDs.

OPEN-SOURCE DOCUMENT OPERATIONS

I-10. Open-source document operations are the systematic extraction of information from publicly available documents in response to command IRs. Open-source document operations can be separate operations or can be included as part of other ongoing operations. Open-source documents are significant in the planning of all operations, especially during the execution

of stability and reconstruction operations and civil support operations. As well as hard data, open-source information can provide valuable background information on the opinions, values, cultural nuances, and other sociopolitical aspects in AOIs. In evaluating open-source documents, collectors and analysts must be careful to determine the origin of the document and the possibilities of inherent biases contained within the document.

CAPTURED DOCUMENT OPERATIONS

I-11. One of the significant characteristics of operations is the proliferation of recordkeeping and communications by digital methods (faxes, e-mails, typed, or computer-generated documents). The rapid and accurate extraction of information from these documents contributes significantly to the commander's accurate visualization of his battlefield. Documents may be captured on or in immediate association with EPWs and detainees, may be found on or turned in by refugees, line crossers, DPs or local civilians, or may be found in abandoned enemy positions or anywhere on the battlefield.

DOCUMENT EVACUATION AND HANDLING

I-12. The rapid evacuation and exploitation of documents is a shared responsibility. It originates with the capturing unit and continues to the complete extraction of pertinent information and the arrival of the document at a permanent repository, normally at the joint level, either within the theater of operations or outside of it. Documents captured in association with detainees and EPWs, with the exception of identity documents, are removed from the individual to ensure that documents of intelligence interest are not destroyed. These documents are evacuated through EPW evacuation channels with, but not on the person of, the detainee. With the exception of official documents, all documents are eventually returned to the detainee.

I-13. CEDs not associated with a detainee are evacuated through MI channels, generally starting with the capturing unit's S2. Depending on the type of documents, they may eventually be evacuated to the National Center for Document Exploitation. HUMINT collectors and translators can extract information of intelligence interest from CEDs at every echelon; they will make an attempt to exploit CEDs within their expertise and technical support constraints. Collectors evacuate CEDs to different elements based upon the information contained and the type of document concerned. For example, documents related to criminal activity may be evacuated to the nearest criminal investigative unit. Direct evacuation to an element outside the chain of command takes place at the lowest practical echelon but is normally done by the first MI unit in the chain of command. Document evacuation procedures are outlined in Annex B (Intelligence) of the unit's OPORD and SOPs.

Actions by the Capturing Unit

I-14. Document accountability begins at the time the document comes into US possession. Original documents must not be marked, altered, or defaced in any way. The capturing unit attaches a DD Form 2745 (Enemy Prisoner of War Capture Tag), Part C, to each document. Only in the case where a

capturing unit does not have the time nor the manpower to mark each document due to ongoing combat operations should the capturing unit fill out one capture tag for a group of documents. In this case, the capturing unit should place the documents in a weatherproof container (box or plastic bag). The capturing unit should fill out two copies of the DD Form 2745, placing one copy inside the container and attaching one to the outside of the container. If these forms are not available, the capturing unit records the required data on any piece of paper. Figure I-1 shows an example of a field expedient tag. At a minimum, the capturing unit should record the information as follows:

- Time the document was captured as a DTG.
- Place document was captured, including an 8-digit coordinate, and description of the location. This should be as detailed as time allows. For example, if a terrorist safe house was searched, documents might be "bagged and tagged" based on what room of the house they were in, what file cabinet, what desk, and so forth.
- Identity of the capturing unit.
- Identity of the source from whom the document was taken, if applicable.
- Summary of the circumstances under which the document was found.

I-15. Document evacuation procedures are listed in Annex B (Intelligence) to the OPORD. If the capturing unit does not contain a supporting HCT, it forwards any CEDs found on the battlefield directly to its S2. The S2 extracts PIR information as practicable, ensures that the documents are properly tagged, and ensures speedy evacuation to the next higher echelon through intelligence channels. Normally, a capturing unit will use any available vehicle, and in particular empty returning supply vehicles, to evacuate documents. Documents captured on or in association with detainees, including EPWs, should be tagged and removed from the detainee. They are evacuated with (but not on) the detainees to an MP escort unit or an EPW holding facility.

I-16. When large numbers of documents are captured in a single location, it is often more expedient for the capturing unit to request a DOCEX team or HCT from the supporting MI unit be sent to the documents rather than attempting to evacuate all the documents. This reduces the burden on the capturing unit, facilitates the rapid extraction of information, and enables the priority evacuation of documents of importance to higher echelons. This method should only be used if the capturing unit can adequately secure the documents until the arrival of the DOCEX team and if the battlefield situation and MI resources permit the dispatch of a team. The capturing unit should include in its request the following:

- The identification of the capturing unit.
- Its location and the location of the documents.

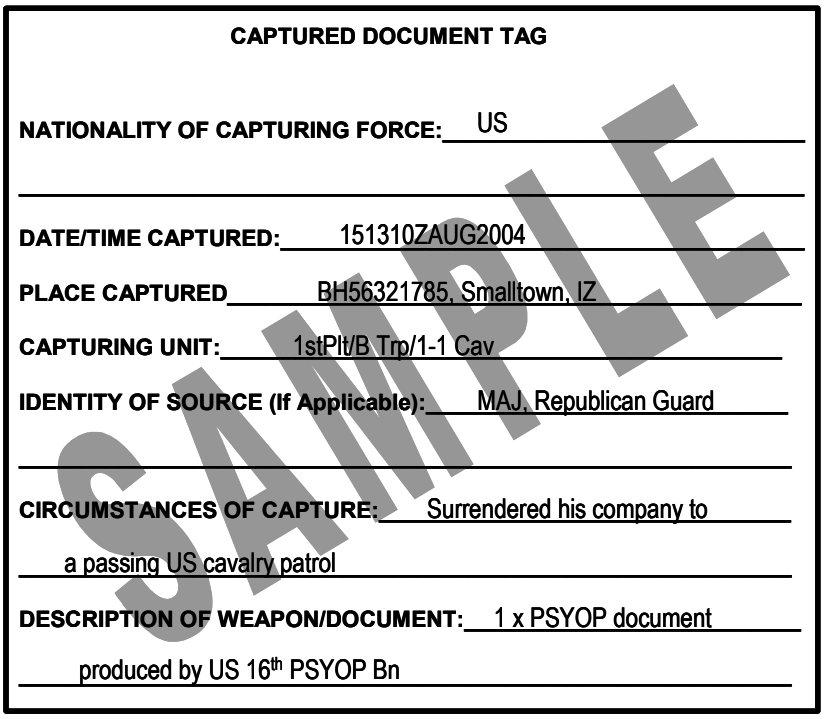


Figure I-1. Example of a Field Expedient Capture Document Tag.

- The general description of the document site (such as an enemy brigade headquarters).
- The approximate number and type of documents.
- The presence of captured computers or similar equipment.

I-17. The MI unit dispatching the team should notify the requesting team as soon as possible to provide them an estimated time of arrival and to coordinate the arrival of the team. There is no set time for how long any particular echelon may keep a document for study. The primary aim of speedy evacuation to the rear for examination by qualified DOCEX elements remains. Each echelon is responsible to prevent recapture, loss, or destruction of the CEDs.

ACTIONS BY THE FIRST HUMINT COLLECTION OR DOCEX UNIT

I-18. The first HUMINT collection or DOCEX unit to receive CEDs should log, categorize, and exploit the documents to the best of its abilities based on METT-TC factors. They should rapidly identify documents requiring special handling or special expertise to exploit and evacuate those documents to the appropriate agencies. The MI unit SOP or OPORD should list special document evacuation requirements and priorities.

Accountability

I-19. The capturing unit and each higher echelon take steps to ensure that they maintain CED accountability during document evacuation. To establish accountability, the responsible element inventories all incoming CEDs. Anyone who captures, evacuates, processes, or handles CEDs must maintain accountability. All CEDs should have completed captured document tags. An incoming batch of documents should include a captured document transmittal. Figure I-2 shows this format. The exact format for a document transmittal is a matter of local SOP, but it should contain the information listed below:

- The identity of the element to which the CEDs are to be evacuated.
- The identity of the unit forwarding the CEDs.
- The identification number of the document transmittal.
- Whether or not CEDs in the package have been screened and the screening category. (If not screened, NA is circled.) Document handlers should package documents that have been screened separately, by category.
- A list of the document serial numbers of the CEDs in the package.

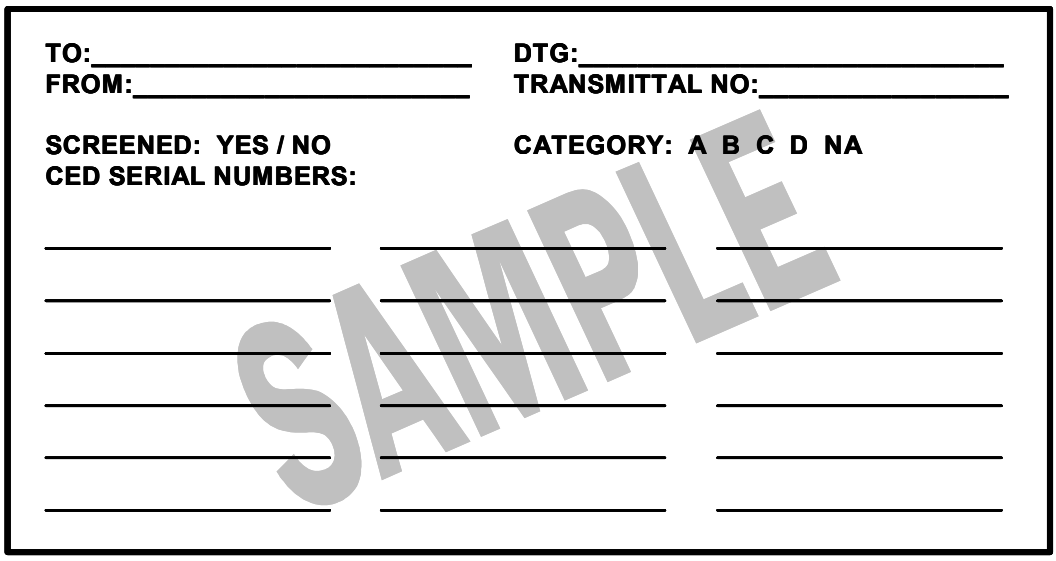


Figure I-2. Example of a Captured Document Transmittal Sheet.

I-20. When a batch is received without a transmittal, the HUMINT collection element contacts the forwarding units and obtains a list of document serial numbers (if possible). The HUMINT collection element records all trace actions in its journal. Accountability includes—

- Inventorying the CEDs as they arrive.
- Initiating necessary trace actions.

- Maintaining the captured document log. (See Figure I-3.)

I-21. When a collector includes intelligence derived from a CED in an intelligence report, he references the identification letters and number of the document concerned to avoid false confirmation.

Inventory

I-22. The receiving element conducts an initial inventory of incoming CEDs by comparing the CED to the captured document tag and accompanying transmittal documents. This comparison identifies—

- Transmittals that list missing CEDs.
- Document tags not attached to CEDs.
- CEDs not attached to document tags.
- CEDs not listed on the accompanying transmittal documents.

UNIT:_____

FILE NUMBER	RECEIVED DOCUMENT DTG SERIAL #	INCOMING TRANSMITTAL#	FORWARDING UNIT	RECEIVED BY	DTG AND PLACE OF CAPTURE
1501	150830AUG99 0102368	1T08	1/82d Abn Div	SSG KIM	150500AUG99/EK030949
1502	150930AUG99 0110443	2T11	2/82d Abn Div	SSG KIM	150620AUG99/EK045860
1503	150930AUG99 1039964	2T11	2/82d Abn Div	SSG KIM	150725AUG99/EK058383
1504	150930AUG99 1192583	2T11	2/82d Abn Div	SSG KIM	150725AUG99/EK058383

CAPTURING UNIT	SCREENING CATEGORY	DESCRIPTION OF DOCUMENT	DESTINATION/ TRANSMITTAL #	REMARKS
Co A, 1/504th, 1 Bde, 82d	A	Letter of promotion, KP, 1Pg	JDEC, 15T01	SALUTE written
Co B, 2/504th, 2 Bde, 82d	A	Letter describing attack, RU, 3 Pg	JDEC, 15T01	SALUTE written
Co B, 2/504th, 2 Bde, 82d	B	List of call signs, RU, 1Pg	JDEC, 15T03	None
Co B, 2/504th, 2 Bde, 82d	C	Personal letter, KP, 2 Pg	JDEC 15T02	Translation end

SAMPLE

Figure I-3. Example of a Captured Document Log.

Trace Actions

I-23. The receiving unit initiates trace actions on all missing CEDs, missing captured document tags, and all information missing from the captured document tags. They initiate trace actions by contacting elements from which the documents were received. The receiving unit can complete this corrective action swiftly if that unit's captured document log was filled out completely. If necessary, the trace action continues to other elements that have handled the document. If a captured document tag is unavailable from elements that have previously handled the CED, the document examiner fills out a

captured document tag for the document using whatever information is available. Attempts to obtain missing CEDs are critical because of the information those CEDs might contain.

Document Logs

I-24. The captured document log is a record of what an element knows about a CED. After trace actions are initiated for any missing documents, the CEDs are entered in the REMARKS section of the captured document log. This log must contain the following:

- Name of capturing unit.
- File number (a sequential number to identify the order of entry).
- DTG the CED was received at this element.
- Document serial number of the captured document tag.
- Identification number of the transmittal document accompanying the CED.
- Complete designation of the unit that forwarded the CED.
- Name and rank of individual that received the CED.
- DTG and place of capture (as listed on the captured document tag).
- Identity of the capturing units (as listed on the captured document tag).
- Document category (after screening).
- Description of the CED. (At a minimum, the description includes the original language; number of pages; type of document such as a map, letter, or photograph; and the enemy's identification number for the CED, if available.)
- Destination and identification number of the outgoing transmittal.
- Remarks to include any other information that can assist the unit in identifying the CED including processing codes. These are set up by local SOPs to denote all actions taken with the document while at the element, including intelligence reports, translations, reproductions, or return of the CED to the source from whom it was taken.

DOCUMENT SCREENING

I-25. Document screening is the rapid but systematic evaluation of documents to determine which documents contain priority information. Selected priority documents will be exploited immediately for PIR information and evacuated expeditiously (often electronically) to a DOCEX facility. Document screening can be done manually (requiring a linguist who is well versed in the current collection requirements) or through the use of scanning devices with key word identification capability. Document processing does not require the complete translation of a document but requires sufficient translation to

determine the significance of the document. A non-linguist may be able to do a degree of preliminary screening based on document format and the location where the document was found.

I-26. As screeners screen each document, they assign one of four category designations. The assigned category determines the document's priority for exploitation and evacuation. Document screening requires that the screening units receive the most current PIR and intelligence requirements; current friendly and enemy situation update; and relevant OB information. Screeners at higher echelons can re-categorize CEDs, to more accurately reflect the requirements at that level or information that has past its LTIOV.

DOCUMENT CATEGORIES

I-27. Documents are divided into categories to prioritize their evacuation and the extraction of information from them for intelligence purposes. Document categories are discussed below.

Category A

I-28. Category A documents are those that require priority evacuation and/or special handling because of their special intelligence value. They contain SALUTE reportable information. Category A documents also include those that are of interest to another command, collecting agency, or other agency (for example, TECHINT, Air Force, Navy, PSYOP, Cryptography).

I-29. What determines if a document is a Category A document changes according to the operational environment and will be set forth in each DOCEX element's SOP and in Annex B (Intelligence) of the unit's OPORD. Documents that are evidence in legal proceedings against captured personnel suspected of crimes against humanity and war crimes will be handled as Category A documents. All Category A documents are handled as SECRET. Standard Category A documents include but are not limited to—

- Unmarked maps.
- Maps and charts containing any operational graphics, which are sent to the G2/S2. From G2/S2, they would be evacuated to the all-source analysis center.
- Air Force related documents, which should go to the nearest Air Force headquarters.
- Navy related documents, which should be sent to the nearest Navy headquarters.
- TECHINT-related documents, which are evacuated to the nearest TECHINT unit.
- Cryptographic and communications-related documents, which are evacuated to the nearest SIGINT analysis unit.
- Documents constituting evidence to be used in legal proceedings against persons suspected of crimes against humanity and war crimes,

which will be marked "CRIMINAL EVIDENCE." Such documents will be kept separate from other documents and will be stored under guard or in a secure area until turned over to a war crimes investigative unit. SJA should be consulted concerning chain of custody requirements.

Category B

I-30. Category B documents contain information of intelligence interest to the supported command. The lowest echelon possible exploits the documents and evacuates them through intelligence channels. Category B documents are handled as SECRET.

Category C

I-31. Category C documents and items contain no information of intelligence interest but still require special administrative accountability (for example, currency, works of art, narcotics). Currency is accounted for on DA Form 4137 (Evidence/Property Custody Document).

Category D

I-32. Category D documents contain no information of intelligence value. Only the theater or higher document repository can categorize documents as Category D.

GROUP DOCUMENTS

I-33. CEDs are first grouped according to their assigned screening category. Personnel must be careful when sorting CEDs to ensure no CED is separated from its associated documents. These large groupings can be broken down into smaller groups. Each of these smaller groupings consists of CEDs that were—

- Captured by the same unit.
- Captured in the same place.
- Captured on the same day at the same time.
- Received at the DOCEX element at the same time.

TRANSMITTAL OF CEDS FROM FIRST AND SUBSEQUENT MI UNITS

I-34. Unless they have an HCT in DS, most units that capture or find documents normally have no way of evaluating, categorizing, or otherwise differentiating documents. They are all tagged and evacuated together by the most expedient means through MI channels. Once these documents arrive at a HUMINT collection or DOCEX unit, the unit can screen, categorize, and extract information from the documents. The degree that documents are exploited at each echelon is dependent on mission priorities and available resources. Document handlers must note any attempts to exploit CEDs on the transmittal documents to prevent unnecessary duplication of effort by higher echelons.

I-35. When transportation assets are limited, CEDs are evacuated according to priority based on document categorization. All Category A CEDs will be evacuated first, followed in order by Categories B, C, and D. Documents that have not yet been screened will be evacuated as Category C documents, but the transmittal slip will clearly indicate that the documents have not been screened.

I-36. Documents will be evacuated in accordance with unit SOP and Annex B (Intelligence) in the unit OPORD. Lower priority CEDs, no matter how old, are never evacuated ahead of those with higher priority. CEDs are packaged so that a package of documents contains CEDs of only one category. If the CED cannot be screened because of time or language constraints, it should be treated as a Category C, but kept separate from screened Category C CEDs.

I-37. When CEDs are evacuated from any echelon, a document transmittal sheet is used (Figure I-2). A separate transmittal document is prepared for each group of CEDs to be evacuated. The sending unit prepares a separate transmittal document for each separate addressee. The transmittal identification number is recorded in the captured document log (Figure I-3) as part of the entry for each captured document. Copies of all translations should accompany the documents to avoid duplication of effort. If the sending unit submitted intelligence reports electronically, it should note the report number or include a copy of the report with the document to avoid duplicate reporting.

I-38. All CEDs being evacuated must be accompanied with the appropriate—

- Technical document (TECHDOC) cover sheet.
- SECRET cover sheet on Categories A and B documents.
- Translation reports and hardcopy reports accompanying translated documents.
- Captured document tags.

JOINT DOCUMENT EXPLOITATION FACILITY

I-39. The Theater MI brigade or group is normally tasked with the establishment of the theater JDEF. The JDEF is staffed by Army linguists, supported by technical experts from the Army and from the other services, and supplemented as required by military and civilian contract translators. The JDEF will normally contain MI experts from SIGINT, CI, TECHINT, and other areas as required to identify and exploit documents of interest to these specialties.

I-40. Military and civilian translators must have security clearances appropriate to their mission requirements. This normally equates to at least a Secret clearance since the translators must be made aware of US collection requirements to facilitate their work. The JDEF performs a final examination of all documents of possible theater intelligence value before storing or evacuating them. The DIA sets procedures for exploitation of documents above theater Army level.

DOCUMENT PROCESSING (RECOVERY AND TRANSLATION)

I-41. Units must normally process documents prior to exploiting them. Document processing includes the translation of foreign language documents into English, the recovery of damaged documents, the decryption of encrypted documents, and the extraction of documents from electronic media such as the extraction or downloading of files from a computer disc or hard drive. This need for processing frequently limits the amount of DOCEX that can be done outside a DOCEX facility.

DOCUMENT RECOVERY

I-42. At a minimum, the JDEF manning includes teams trained in extracting and downloading information from electronic media such as computer hard drives. These individuals work in conjunction with TECHINT personnel responsible for the evaluation of captured computer hardware and software. These teams are prepared to deploy forward as necessary to accomplish their mission.

DOCUMENT TRANSLATION

I-43. Translations are not intelligence information reports. They are, however, often a precondition for DOCEX. Once translated, intelligence information can be extracted and reported on an IIR, SALUTE, or similar report. A translation should accompany the original foreign language document; a copy of the translation should accompany any copies of the original foreign language document and, as required, the intelligence reports. A translation report should contain the following information:

- Where the report will be sent.
- Which element prepared the report.
- DTG of the document translation.
- Report number as designated by local SOPs.
- Document number taken from the captured document tag.
- Document description including type of document, number of pages, physical construction of document, and enemy identification number, if applicable.
- Original captured document language.
- DTG document was received at element preparing the report.
- DTG document was captured.
- Place document was captured.
- Identity of capturing unit.
- Circumstances under which document was captured.
- Name of translator.

- Type of translation: full, extract, or summary.
- Remarks for clarification or explanation, including the identification of the portions of the document translated in an extract translation.
- Classification and downgrading instructions in accordance with AR 380-5.

TYPES OF TRANSLATION

I-44. There are three types of translations:

- Full—one in which the entire document is translated. This is both time and manpower intensive, especially for lengthy or highly technical documents. Normally only a DOCEX facility at theater or national level will do full translations, and then only when the value of the information, technical complexity, or political sensitivity of the document requires a full translation. Even when dealing with Category A documents, it may not be necessary to translate the entire document to gain the relevant information it contains.
- Extract—one in which only a portion of the document is translated. For instance, a TECHINT analyst may decide that only a few paragraphs in the middle of a 600-page helicopter maintenance manual merit translation, and that a full translation is not necessary. The analyst would request only what he needed.
- Summary—one in which a translator begins by reading the entire document. He then summarizes the main points of information instead of rendering a full or extract translation. A summary translation is normally written, but may be presented orally, particularly at the tactical level. Summary translations may be done as part of the document screening process. A summary translation requires a translator have more analytical abilities. The translator must balance the need for complete exploitation of the document against time available in combat operations. Translators working in languages of which they have a limited working knowledge may also use a summary translation. For instance, a Russian linguist may not be able to accurately deliver a full translation of a Bulgarian language document. However, he can probably render a usable summary of its content.

TRANSLATOR SUPPORT TO DOCEX

I-45. When HUMINT collectors are not available due to shortages or other mission requirements, DOCEX can be performed by military or civilian linguists under the management of a cadre of HUMINT collectors.

SECURITY REQUIREMENTS

I-46. Document translators will usually need to have a clearance in order to conduct document translation. An exception is that open-source document translation does not require a security clearance unless the information collected from the open-source documents is linked to specific US collection

requirements, plans, or operations. In this case the translator will need a clearance appropriate to the level of the particular contingency plan or operation to which the information is linked. Individuals without a security clearance should not be used in the exploitation of a closed source or CEDs. By their very nature, the translation of these documents gives keys into the level of US knowledge and the direction of US planning and intentions that precludes their translation by individuals without a security clearance.

SOURCES OF TRANSLATORS

I-47. There are various sources that a commander can use to obtain the linguists necessary to support DOCEX operations.

- RC and AC MI linguists. Dependent on their mission requirements, any MI soldiers with the required language qualification may be used as document translators. The advantage of using MI soldiers is that they have the appropriate security clearance and have a firm grasp of collection requirements. The DOCEX operation will usually require MI officers to manage the administrative portions.
- Other linguists. Non-MI Army linguists include numerous soldiers who have proficiency in a foreign language, regardless of MOS. US civilians can be contracted to provide translator support as can local nationals. Local national hires will provide the bulk of the translator support.

REQUIREMENTS FOR A DOCEX OPERATION

I-48. The number of personnel required to conduct DOCEX varies with the echelon and with the volume of documents. Regardless of the size of the operation, certain basic functions must occur:

- Supervision and Administration. These are the C2 and logistical aspects of the DOCEX operation that ensure that operations are smooth and uninterrupted.
- Accountability. Accountability includes logging documents in and out, copying documents as required, storing documents, receiving and transmitting documents, maintaining files, and other routine activities. This ranges from a parttime task for one individual at a low echelon, to warehouse-sized operations involving tons of documents at an EAC document repository.
- Screening. Screening involves the review and categorization of all documents, the prioritization for translation and exploitation, and the identification of documents for special handling and immediate transmittal to specialized units for exploitation. Screening requires senior, experienced individuals well versed in the target language and the collection requirements, capable of making rapid decisions based on minimal information. The number of screeners required depends on the document flow that may range from only a few per day at a low echelon, to literally thousands of documents a day at a theater-level activity.

- Security Requirements. Security requirements include ensuring that the personnel dealing with the documents have the appropriate security level and that they do not pose a security risk to the US. This is particularly important when dealing with non-US translators. Security also evolves ensuring that the documents are marked in accordance with regulation and that proper security measures are in place to prevent compromise of information. At higher echelons, dealing with large numbers of non-US translators normally requires a designated CI team conducting recurring personnel security evaluations.
- Translation. This function involves the directed translation of documents from the target language to English. It requires personnel with the appropriate clearance level who have a working idiomatic knowledge of the target language and English. Higher echelon activities, such as the EAC document repository, group their translation efforts by subject area. For example, one person or group could translate all medical-related documents. At lower echelons, the translators require a more general knowledge. At lower echelons, the same person may translate a document, extract the pertinent information, and report that information. At higher echelons, these are often separate functions.
- Exploitation and Reporting. This task is the identification and extraction of information in response to collection requirements and requires a high level of expertise. The individual must be totally knowledgeable of collection requirements and must be able to readily identify indicators of activity or identify the significance of minute pieces of information that could contribute to answering requirements. Reporting involves placing that extracted information into a coherent, properly formatted report so that the all-source analyst can add it to the intelligence picture.
- Quality Control. This aspect includes ensuring that all aspects of the DOCEX operation—including accounting for, screening, translating, exploiting, and reporting—are functioning correctly.

REPORTING

I-49. Information collected from documents is normally reported in a SALUTE report or an IIR. Reporting through other reporting formats is discouraged. Intelligence reports are normally forwarded electronically or as otherwise directed by SOPs and operational instructions. Normally an electronic or hardcopy file of each report is maintained at the unit of origin; one electronic or hardcopy is submitted through intelligence reporting channels; and one is forwarded with evacuated documents to the next unit to receive the document to prevent redundant reporting. In the event that the document itself cannot be evacuated in a timely manner, a verified copy of a translation report can be forwarded separately from the original document to an exploitation agency.

DOCUMENT EXPLOITATION IN SUPPORT OF HUMINT COLLECTION

I-50. Documents found on detainees, including EPWs—that can be exploited more efficiently when combined with HUMINT collection—are forwarded with the detainee to the next echelon in the EPW/detainee evacuation channel. In exceptional cases, documents may be evacuated ahead of the EPW or other detainee for advance study by intelligence units. A notation should be made on the EPW's capture tag or accompanying administrative papers about the existence of such documents and their location if they become separated from the detainee.

SOURCE-ASSOCIATED DOCUMENTS

I-51. Documents captured on or in association with a human source play an important role in the HUMINT collection process. These documents may contain reportable information the same as with any other CED. The information is immediately extracted from the documents and forwarded in the appropriate intelligence report. In addition to reportable information, documents (in particular personal documents) may provide valuable insight into the attitude and motivation of the source and can be effectively used by the HUMINT collector in the approach process (see Chapter 8). Guidelines for the disposition of the detainee's documents and valuables are set by international agreements and discussed in more detail in AR 190-8 and FM 19-4.

I-52. The capturing unit removes all documents, with the exception of the source's primary identification document, from an EPW or other detainee to prevent their destruction. These are placed in a waterproof container (usually a plastic bag) and Part C of the capture tag is placed in the bag. Documents from each source should be placed in a separate bag. These documents are turned over to the first MP EPW handling unit in the chain of command. The MPs will inventory all documents and prepare a handreceipt and provide a copy to the EPW or detainee.

I-53. To ensure proper handling and expeditious disposition of these documents, the first HUMINT collection element to see the detainee should review the documents as part of the source screening process. If an official document is confiscated and evacuated through MI channels, the HUMINT collector must obtain a receipt for that document from the MPs. If possible, the HUMINT collection unit copies any documents that contain information of intelligence interest and forwards the copies through MI channels. With the exception of an identification document, documents are normally kept separate from the detainee until the detainee arrives at a permanent confinement facility, at which time documents are returned to them per AR 190-8.

I-54. Three possible actions may be taken with documents captured with a source. The documents may be confiscated, impounded, or returned to the source.

Confiscated

I-55. Documents confiscated from a source are taken away with no intention of returning them. Official documents, except identification documents, are confiscated and appropriately evacuated. The intelligence value of the document should be weighed against the document's support in the HUMINT collection of the source. The HUMINT collector must comply with the accounting procedures established for CEDs by the MPs in accordance with AR 190-8.

Impounded

I-56. Some CEDs will contain information that must be exploited at higher echelons. These documents may be impounded by the HUMINT collector and evacuated through intelligence channels. The HUMINT collector must issue a receipt to the source for any personal documents that he impounds. He must comply with the accounting procedures established for CEDs impounded by the MPs in accordance with AR 190-8. When a CED is impounded, it is taken with the intent of eventual return. Personal documents with military information will be impounded if the military value is greater than the sentimental value. An example of a personal document whose military value might outweigh the sentimental value could be a personal photograph that includes military installations or equipment.

I-57. When a CED is impounded, it must be receipted. The receipt will include an itemized list of all the items taken from the prisoner, and the name, rank, and unit of the person issuing the receipt. Items of high value may be impounded for security reasons. For instance, an EPW or detainee apprehended with an unusually large amount of money would have the money impounded and receipted. The MPs will establish and maintain a DA Form 4237-R (Detainee Personnel Record) for impounded items. The register will identity the owner of the impounded items and provide a detailed description of the items impounded. A receipt will be given to anyone who has items impounded. Also, the OIC or authorized representative will complete and sign DA Form 1132-R (Prisoner's Personal Property List – Personal Deposit Fund). A copy will be provided the source. See AR 190-8 for procedures on handling personal effects.

Returned

I-58. Returned CEDs are usually personal in nature. They are taken only to be inspected for information of interest and are given back to the source. Personal documents belonging to a source will be returned to the source after examination in accordance with the GPW. These documents are CEDs whose sentimental value outweighs their military value and may be returned to the source. Copies of these documents may be made and forwarded if deemed necessary. Except for an identification document (which is always returned to the source), documents are evacuated with the source, rather than on the source, until the source reaches a permanent confinement facility at EAC.

This page intentionally left blank.

Appendix J

References

The following references are provided to assist HUMINT collectors, commanders, and trainers in obtaining regulatory guidance for HUMINT collection operations. These and other references are in the bibliography.

1. AR 350-1. *Army Training and Education.* 9 April 2003.
2. AR 380-5. *Department of the Army Information Security Program.* September 2000.
3. AR 380-10. *Technology Transfer, Disclosure of Information, and Contacts with Foreign Representatives.* 15 February 2001.
4. AR 380-15. *(C) Safeguarding NATO Classified Information.* 1 March 1984.
5. AR 380-28. *Department of the Army Special Security System*. 12 December 1991.
6. AR 380-40. *Policy for Controlling and Safeguarding Communications Security (COMSEC) Material.* 22 October 1990.
7. AR 380-49. *Industrial Security.* 15 April 1982.
8. AR 380-53. *Telecommunications Security Monitoring*. 29 April 1998.
9. AR 380-67. *Personnel Security Program*. 9 September 1988.
10. AR 381-1. *Security Controls on Dissemination of Intelligence Information.* 12 February 1990.
11. AR 381-10. *U.S. Army Intelligence Activities*. 1 July 1984.
12. AR 381-12. *Subversion and Espionage Directed Against the US Army (SAEDA).* 15 January 1993.
13. AR 381-14. *Technical Counterintelligence (TCI).* 30 September 2002.
14. AR 381-20. *(U) US Army Counterintelligence Activities (S).* 26 September 1986.
15. AR 381-45. *Investigative Records Repository*. 25 August 1989.
16. AR 381-47. *(U) US Army Offensive Counterespionage Activities (S).* 30 July 1990.
17. AR 381-100. *(U) Army Human Intelligence Collection Program (S).* 15 May 1988.
18. AR 381-102. *(U) US Army Cover Support Program (S).* 10 January 1991.
19. AR 381-143. *Military Intelligence Nonstandard Material Policies and Procedures.* 1 December 1986.

20. AR 381-172. *Counterintelligence Force Protection Source Operations and Low-Level Source Operations*. 30 December 1994.

21. AR 614-115. *Military Intelligence Excepted Career Program*. 12 April 2004.

22. AR 614-200. *Military Intelligence Civilian Excepted Career Program*. 30 September 2004.

23. DA Pam 381-15. *Foreign Military Intelligence Collection Activities Program*. 1 June 1988.

24. Executive Order 12333. *United States Intelligence Activities*. 4 December 1981.

25. DOD Directive 2310.1. *DOD Program for Enemy Prisoners of War (EPOW) and Detainees (Short Title: DOD Enemy POW Detainee Program)*. 18 August 1994.

26. DOD Directive 3115.09. *DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*. 3 November 2005.

27. DOD Directive 5100.77. *DOD Law of War Program*. 9 December 1998.

28. DOD Directive 5240.1. *DOD Intelligence Activities*. 3 December 1982.

29. DOD Instruction 3020.41. *Contractor Personnel Authorized to Accompany the U.S. Armed Forces*. 3 October 2005.

30. The Under Secretary of Defense for Intelligence (USD(I) Memorandum, *Guidance for the Conduct and Oversight of Defense Human Intelligence (HUMINT) (U)*. 14 December 2004.

31. USD(I) Memorandum, Implementation Instructions for USD(I) Memorandum, *Guidance for the Conduct and Oversight of Defense Human Intelligence HUMINT* (U). 7 September 2005.

32. DOD Regulation 5240.0-R. *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons*. December 1982.

33. Detainee Treatment Act of 2005, Public Law No. 109-163, Title XIV.

Further information and links to many of the above publications can be found at: http://www.dami.army.pentagon.mil/offices/dami-cd/

ARTEPS, MTPs, and other intelligence training products are available at the Reimer Digital Library http://www.adtdl.army.mil.

Appendix K

Contract Interrogators

INTRODUCTION

K-1. Contractors are used increasingly to augment existing capabilities and bridge gaps in the deployed force structure. With the increased use of contractors comes the need to identify the doctrine and procedures affecting their employment. Leaders and those working with contractors must understand that contractors are civilians authorized to accompany the force in the field and should be provided with an ID card as proof of their authorization. In accordance with GPW Article 4, contractors are to be accorded POW status if captured.

KEY TERMS

K-2. **Contract Interrogator.** A contract interrogator is a contractor who is specifically trained and DOD certified for, tasked with, and engages in the collection of information from individuals (HUMINT sources) for the purpose of answering intelligence information requirements. Their operations must be conducted in accordance with all applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. Contract interrogators will operate only in fixed facilities and not in tactical operations. See DOD Instruction 3020.41 for additional information.

K-3. **External Support Contractor.** Contract interrogators fall into the category of External Support Contractor**.** They work under contracts awarded by contracting officers serving under the command and procurement authority of supporting headquarters outside the theater. Their support augments the commander's organic capability.

K-4. **Contracting Officer Representative (COR).** A COR is the contracting officer's designated representative who assists in the technical monitoring and administration of a contract. Typically, a COR is responsible for assisting the contracting officer in contractor-employee day-to-day management of issues that may affect contractor or unit requirements.

K-5. Statement of Work (SOW) or Performance Work Statement:

- Contractor roles and functional requirements, as well as security issues and the relationship to the military chain of command, must be accurately and adequately defined in the SOW. The SOW should include a description of the essential service and require the contractor

to prepare contingency plans to reasonably ensure continuation. Contractors are required to perform all tasks identified within the SOW and all other provisions defined within the contract. The SOW may also stipulate the appointment of a senior contractor at each echelon or facility to be the point of contact for the commander and the COR for resolving contract performance and scheduling challenges.

- The contract must stipulate whether the duty of a senior contractor is an additional duty or the full-time job of the selected contractor. Considering that contractors are "managed" rather than "commanded," having a senior contractor will assist the commander in managing the contract. Without an onsite contractor supervisor, the default chain of command for contract interrogators might otherwise reside in CONUS, at the contractor's headquarters.

CIVILIAN STATUS

K-6. A contract employee cannot be made to engage in any activity inconsistent with his civilian status such as serving as a crew member on a weapon system. Interrogations are presumptively consistent with civilian contractor status, but other tasks should be vetted with the command's legal advisor to ensure they are legally permissible.

COMMAND CONSIDERATIONS

K-7. Theaters in which large-scale operations are conducted are very likely to employ contract interrogators, due to limited numbers of Army HUMINT collectors available. The presence of contractors in the AO adds an additional dimension to the commander's planning process. Force protection is a critical issue. Even in "permissive" environments such as in the case of humanitarian operations, contractors may be placed in danger. The commander must protect his contractors since they have limited capacity to protect themselves.

K-8. The commander has no command authority over contractor personnel. Their relationship with the Government is governed by the terms and conditions of their contract. In short, the commander must "manage" contractor personnel through the contracting process. He has no authority to command or discipline them unless it is a declared war, at which time contractors may fall under the provisions of the UCMJ. This distinction between command and management does not prohibit the commander from directing contractors to carry out essential activities, such as activities related to security and safety, consistent with the terms of their contracts.

K-9. The terms and conditions of any contract must be constructed so as to include provisions requiring contractor personnel to abide by all guidance and obey all instructions and general orders applicable to US Armed Forces and DOD civilians including those issued by the Theater Commander. The contractor can be required to "take reasonable steps" to ensure his personnel comply with the above and to ensure "the good conduct" of his employees. Furthermore, the contractor can be required to promptly resolve, to the satisfaction of the COR, all contractor employee performance and conduct problems identified by the COR. The COR can direct the

contractor, at the contractor's expense (for example, a non-allowable charge to the contract) to remove and replace any contractor employee failing to comply with the above. This provides a significant tool to aid in achieving good order and discipline within an AO. The commander also has the authority to initiate proceedings that could lead to charges under Military Extraterritorial Jurisdiction Act (MEJA) or the War Crimes Act.

K-10. Contractors will be subject to the extraterritorial jurisdiction of the United States and will comply with all applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. Contractor misconduct may be subject to prosecution under federal jurisdiction pursuant to the MEJA or the War Crimes Act, or both. Procedures for initiating investigation into such misconduct will normally be established by the operational command.

K-11. The operational command will also establish procedures for referral to federal civilian authorities and necessary pre-trial confinement. Contractors normally will also be subject to the criminal jurisdiction of the HN unless granted immunity from jurisdiction through the provisions of a SOFA or equivalent agreement, or unless the HN waives jurisdiction. As a general rule, contractors are not subject to the UCMJ (with the possible exception for periods of formally declared war).

K-12. The commander should expect contractors to use all means at their disposal to continue to provide essential services, in accordance with the terms and conditions of contracts, until the military releases them. The combatant commander determines when to execute contingency plans for essential services and when to release a contractor.

INTERROGATOR CONTRACT CONSIDERATIONS

K-13. Contracts should be written with the following principles and considerations:

- Contractors will be deployable under all operational scenarios. They will be subject to the same time-phased force deployment data requirements as deploying military units.
- The contractor information system will interface with the Standard Army Management Information System at both retail and wholesale levels. Army units should not have to contend with two separate information systems.
- The contractors will provide interrogation support at fixed facilities as needed. During deployments, the commander (subject to contract terms and conditions) will determine where contractors operate in their AO.
- The contractors will not replace force structure. They will augment Army capabilities and provide an additional option for meeting support requirements.

- Force protection, including the protection of contractors, is the responsibility of commanders.
- The unit must integrate contractor support into the overall support plan. Transportation of contractors on the battlefield must be planned.
- Command and control of contract personnel is dependent upon terms and conditions of the contract. The contracting officer or his designated representative is the appointed liaison for monitoring contractor performance requirements and will ensure that contractors move material and personnel according to the combatant commander's plan. A good technique is for the command to designate and train a unit COR or Contracting Officer's Technical Representative (COTR) at each facility where contract interrogators will be working. Because international and domestic law, including SOFAs, affect the relationship between commanders and contract personnel, commanders and CORs should seek legal advice concerning issues arising during operations.
- The unit must establish a contractor personnel reporting and accountability system. Again, a good technique is for the command to designate and train a unit COR or TCOR at each facility where contract interrogators will be working.
- During deployments, contractors will live and work in field conditions comparable to those for the supported ARFOR. Living arrangements, transportation requirements, food, medical, and other support services will be provided according to the contract. These services may include but are not limited to—
 - Non-routine medical and dental care.
 - Mess.
 - Quarters.
 - Special clothing, equipment, weapons, or training mandated by the applicable commander.
 - Mail.
 - Emergency notification.
- Planning must be accomplished to ensure agreed upon support to contractors is available to the responsible commander.

CONTRACT INTERROGATOR REQUIREMENTS

SELECTION AND EMPLOYMENT CRITERIA

K-14. Contract personnel must meet certain minimum requirements to be qualified to work as contract interrogators. It is the responsibility of the hiring contracting company to ensure that these criteria, set by the Government, are met by the personnel they hire.

K-15. Policy will dictate employment criteria such as minimum education, military service, security clearance, and previous training. Certain civilian experience and training may also meet the policy requirements for contract

interrogator qualifications. Commanders and CORs should refer to the current DA policy on contract interrogators for appropriate guidance.

TRAINING REQUIREMENTS

K-16. All contractor interrogators must successfully complete a training program approved by the United States Army Intelligence Center and Fort Huachuca, or the Defense HUMINT Management Office, which will serve as validation to perform MI interrogations (see DODD 3115.09). The organization Commander or Director initiating the contract must certify that the training has been completed. The training program will ensure that contract interrogators are trained and certified on—

- The most current TTP of interrogation as promulgated by DOD.
- The applicable law and policy related to the treatment of detainees. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs.

K-17. Contract interrogators must also receive training on the supported unit's mission and Interrogation Counter-Resistance Policy pertinent to the AOR they are supporting. This training will be conducted in-theater by the gaining unit.

EQUIPMENT

K-18. Contractors must be issued personal protection gear appropriate for the threat environment. This may include ballistic helmet, personal body armor, NBC protective gear, and in certain circumstances a personal weapon. Contract interrogators must have access to automation equipment to support their mission of intelligence collection and reporting.

UTILIZATION

K-19. Only trained and certified contractors working under the supervision of MI personnel are authorized to conduct interrogations. Contract interrogators may conduct interrogations with an interpreter in the room; however, an OIC or NCO will monitor the interrogation by personal presence or by means of live video camera feed.

K-20. Contract interrogators—

- Will not supervise any military personnel or federal government employees, nor will they be in charge of interrogation facilities.
- Will operate only in fixed facilities. This requirement provides a measure of force protection to the contract interrogator and frees up Army HUMINT collectors for tactical missions.
- Must submit a written interrogation plan to the OIC or NCOIC, and receive approval for the plan, in advance of each interrogation. The plan will specify the information desired and identify what techniques

and approaches for obtaining information will be used to conduct the interrogations.

WORK LOCATIONS

K-21. The commander may position contract interrogators in fixed detention facilities anywhere in the theater, in accordance with the terms and conditions of their contract.

ATTIRE

K-22. Contractors accompanying the force should be visibly distinct from soldiers so as not to jeopardize their status. The JTF or combatant commander may direct contract personnel to wear civilian clothing or a uniform that says "civilian." Specific items of military attire required for safety or security may also be worn, such as chemical defense equipment, cold weather equipment, or mission specific safety equipment.

FIRE ARMS

K-23. A contractor authorized to accompany the force in the field is *not entitled* to be issued a firearm. However, a contract employee may be armed only if **all** of following conditions are met:

- The theater commander grants his approval.
- The employee's corporate policy allows it.
- The employee agrees.

K-24. If all three conditions are met, then the employee must pass proper military side-arm training and will be issued a military specification weapon and ammunition (generally, a 9-millimeter pistol) for *personal protection*. The contractor must also comply with all applicable DOD, service, and local command policies on weapons.

RECOMMENDED READING

DOD Instruction 3020.41. *Contractor Personnel Authorized to Accompany the U.S. Armed Forces.* 3 October 2005.

AR 715-9. *Contractors Accompanying the Force*. 29 October 1999.

DA Pamphlet 715-16. *Contractor Deployment Guide*. 27 February 1998.

FM 3-100.21. *Contractors on the Battlefield*. 3 January 2003.

FM 63-11. *Logistics Support Element Tactics, Techniques, and Procedures*. 8 October 1996.

AMC Pamphlet 715-18. *AMC Contracts and Contractors Supporting Military Operations*. June 2000.

Appendix L

Sample Equipment for HCT Operations

L-1. This materiel and equipment list is provided as a sample of what an HCT may require to support the commander's intelligence requirements. Some of the equipment that is intended to be given to a source should be considered expendable.

L-2. HCT Kit Bag - Assumes four-person configuration for each echelon. Regardless of support relationship (Organic/DS/GS/GSR), HCTs inherently require the following.

L-3. Movement/Survivability/Security:

- Two M998 1-¼ ton vehicle (or non-tactical vehicle as appropriate for mission) per team.
- One crew/squad served weapon per team.
- One M16A2 per team.
- Three M4s per team.
- Four 9mms per team.
- M68 Aim-point System.
- One x body armor with protective plate per team member.

L-4. Collection and Reporting System - Hardware 1 x System per HCT:

- Scaleable collection and reporting tool that changes configuration depending on where it is on the battlefield.
- Should include an individual collection and reporting tool.
- Should include a tool for stand-alone SIPRNET connectivity via satellite or other.

L-5. Collection and Reporting System - Software 1 x per System:

- Simple, intuitive Graphic User Interface (GUI).
- Standardized Reports - SALUTE, IIR, Tactical Interrogation Report, Contact Report, BSD Report. (Policy states that once filled out, the BSD becomes classified; therefore, change policy or make the collection or reporting tool classified as well.)
- Source Management Tool.
- CI Investigations Reports.
- Link Analysis (capable of interface with coalition systems—in this case, Analyst Notebook).
- Mapping - Single, standardized tool (down to 1:12,500 scale maps, operational graphics, GPS interface).

- Biometrics Integration/Biometrics Enrollment Tools (Integrated Automated Fingerprint Identification System [IAFIS]-compliant 10-print fingerprint scanners, iris scanners, photographing station).
- Basic DOCEX application.
- Foreign Language Translation.
- Mission Planning Software.
- Query Tools: basic, advanced, multi-entity, multi-media, save user-defined queries.

L-6. Collection and Reporting System - Peripherals 1 x HCT:

- Digital video/still.
- Printer with print and scanner head (photo quality with ports for flash cards/memory sticks).
- Separate collection kit for biometrics (ink/card packets and/or IAFIS-compliant live scanner, iris scanner). Must be FBI compliant and portable).
- GPS.
- Digital voice recorder (Universal Serial Bus [USB] interface).

L-7. Communications - Requires organic communications systems to higher and laterally (non-line of sight and line of sight):

- Intra-team communications - 1 x individual:
 - Secure or nonsecure (prefer secure).
 - Hands-free and/or handheld.
- Team to all - 1 x HCT:
 - Secure.
 - FM/UHF/Microwave.
 - Line of sight.
 - Non-line of sight.
 - Voice.
 - Digital.
 - Cellular telephone:
 - Voice.
 - Backup for transmitting data.
 - GPS enabled.
 - Friendly force identification and tracking system.
- HCT to Source - 2 sets x HCT:
 - Phone cards.
 - Cell phones.
 - Radios.
 - Email or “Blackberry-like” communications.
 - One-way pager.
 - Clandestine signaling.

L-8. Source Support - 2 sets x HCT:

- Source tracking (blue-force tracker-like capability).
- Digital Voice Recorder (micro, USB interface).
- Digital video or still camera, with telephoto lenses.
- GPS.
- 1 x 1Gb Thumb Drive.

L-9. Data Storage - 1 x HCT:

- 2 x hard drives (one for UNCLASS, one for SECRET).
- 2 x Micro/Thumb, 1Gb drive (one for UNCLASS, one for SECRET).

L-10. Power Generation - 1 x liquid fuel generator or high-capacity (12-hour) (battery - silent, vehicle recharge), power source - 1 x HCT.

L-11. 1 x Universal Power Conversion Kit per HCT and OMT.

L-12. Vision Enhancement:

- 2 x night vision goggles (NVG) per HCT.
- 1 x thermal sensor per HCT.
- 1 x binoculars per individual (4 each).
- 1 x laser range finder per HCT.

This page intentionally left blank.

Appendix M

Restricted Interrogation Technique – Separation

INTRODUCTION

M-1. As part of the Army's efforts to gain actionable intelligence in the war on terrorism, HUMINT collectors may be authorized, in accordance with this appendix, to employ the separation interrogation technique, by exception, to meet unique and critical operational requirements. The purpose of separation is to deny the detainee the opportunity to communicate with other detainees in order to keep him from learning counter-resistance techniques or gathering new information to support a cover story; decreasing the detainee's resistance to interrogation. Separation, further described in paragraphs M-2 and M-28, is the only restricted interrogation technique that may be authorized for use. Separation will only be used during the interrogation of specific unlawful enemy combatants for whom proper approvals have been granted in accordance with this appendix. However, separation may **not** be employed on detainees covered by Geneva Convention Relative to the Treatment of Prisoners of War (GPW), primarily enemy prisoners of war (EPWs). The separation technique will be used only at COCOM-approved locations. Separation may be employed in combination with authorized interrogation approaches—

- On specific unlawful enemy combatants.
- To help overcome resistance and gain actionable intelligence.
- To safeguard US and coalition forces.
- To protect US interests.

GENERAL

M-2. This appendix provides doctrinal guidance for the use of separation as an interrogation technique. Separation involves removing the detainee from other detainees and their environment, while still complying with the basic standards of humane treatment and prohibitions against torture or cruel, inhuman, or degrading treatment or punishment, as defined in the Detainee Treatment Act of 2005 and addressed in GPW Article 3 (Common Article III). Separation is to be distinguished from segregation, which refers to removing a detainee from other detainees and their environment for legitimate purposes unrelated to interrogation, such as when necessary for the movement, health, safety and/or security of the detainee, or the detention facility or its personnel. This appendix—

- Will be reviewed annually and may be amended or updated from time to time to account for changes in doctrine, policy, or law, and to address lessons learned.
- Is not a stand-alone doctrinal product and must be used in conjunction with the main portion of this manual.

M-3. Careful consideration should be given prior to employing separation as an interrogation technique in order to mitigate the risks associated with its use. The use of separation should not be confused with the detainee-handling techniques approved in Appendix D. Specifically, the use of segregation during prisoner handling (Search, Silence, Segregate, Speed, Safeguard, and Tag [5 S's and a T]) should not be confused with the use of separation as a restricted interrogation technique.

M-4. Members of all DOD Components are required to comply with the law of war during all armed conflicts, however such conflicts are characterized, and in all other military operations. Proper application of separation as a restricted interrogation technique in selective cases involving specific unlawful enemy combatants and in accordance with the safeguards outlined in this manual is consistent with the minimum humane standards of treatment required by US law, the law of war; and does not constitute cruel, inhuman, or degrading treatment or punishment as defined in the Detainee Treatment Act of 2005 and addressed in GPW Common Article III.

M-5. Use of separation for interrogation is authorized by exception. Separation will be applied on a case-by-case basis when there is a good basis to believe that the detainee is likely to possess important intelligence and the interrogation approach techniques provided in Chapter 8 are insufficient. Separation should be used as part of a well-orchestrated strategy involving the innovative application of unrestricted approach techniques. Separation requires special approval, judicious execution, special control measures, and rigorous oversight.

M-6. Additionally, the use of separation as a restricted interrogation technique shall be conducted humanely in accordance with applicable law and policy. Applicable law and policy for purposes of this appendix include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs.

M-7. More stringent than normal safeguards must be applied when using the separation technique. Use of separation is subject to USD(I) oversight. Compared to approach techniques, there are two additional steps in the approval process (see Figure M-l) for the use of the separation technique:

- First, the COCOM Commander approves (after SJA review) use of the separation technique in theater.
- Second, following the COCOM Commander's approval, the first General Officer/Flag Officer (GO/FO) in an interrogator's chain of command approves each specific use of separation and the interrogation plan that implements separation (this is non-delegable). Interrogation supervisors shall have their servicing SJA review the interrogation plan before submitting it to the GO/FO for approval.

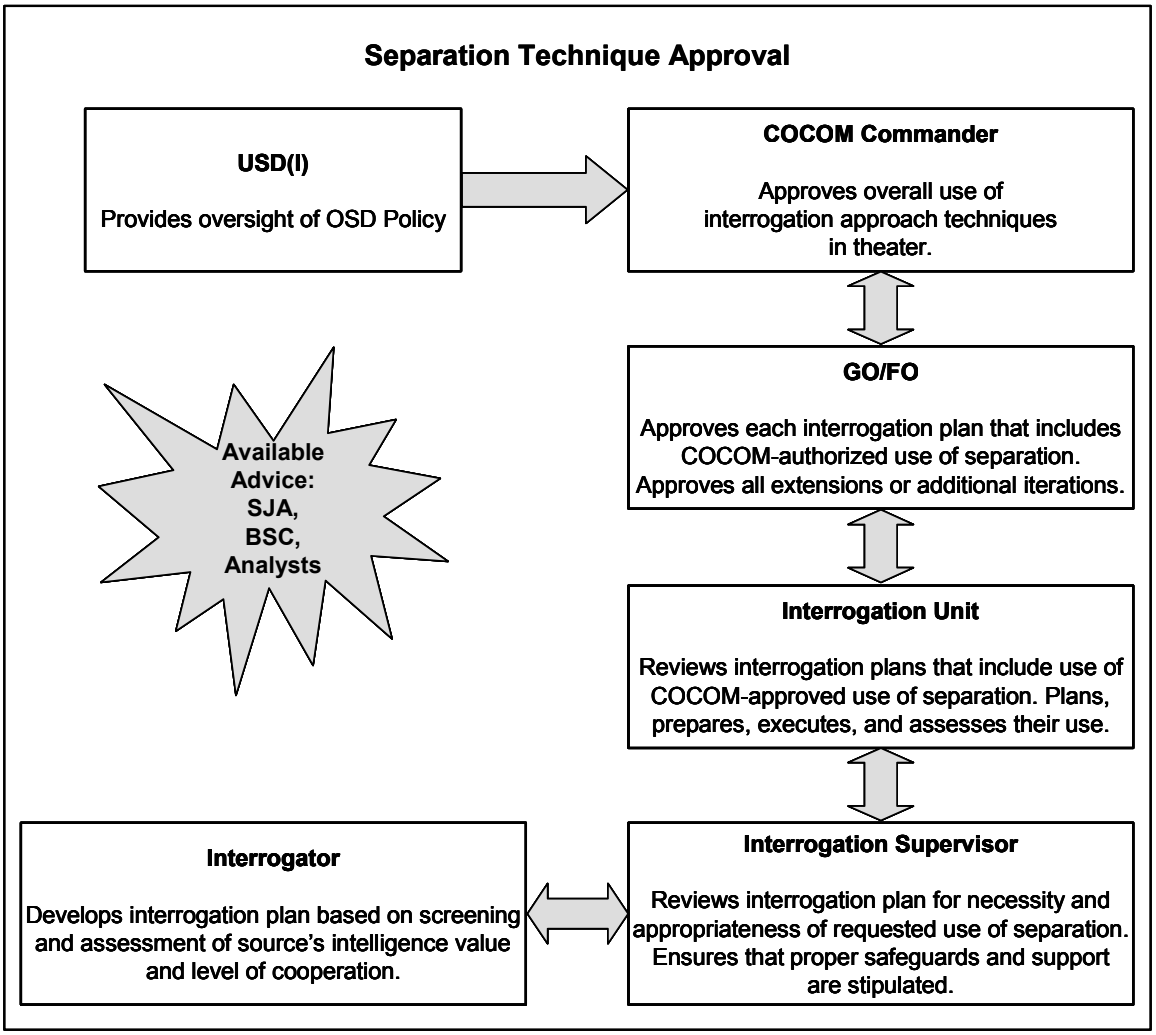


Figure M-1. Separation Approval Process.

M-8. The employment of separation requires notification, acknowledgment, and periodic review, in accordance with USD(I) Memorandum, "(S//NF) Guidance for the Conduct and Oversight of Defense Human Intelligence (HUMINT) (U)," dated 14 December 2004. This means that after the separation is approved for use by COCOMs, the I&WS must be notified as soon as practical. The Office of the Secretary of Defense will review these activities periodically in accordance with DOD Directive 3115.09.

M-9. The planning process for the employment of standard interrogation operations also applies to the employment of the separation technique (see Chapter 4).

RESPONSIBILITIES

M-10. Commanders of interrogation or detention facilities and forces employing the approved separation technique are responsible for compliance with applicable law and policy. Commanders must understand that separation poses a higher risk to the detainee than do standard techniques, and so require strenuous oversight to avoid misapplication and potential abuse.

M-11. The interrogation chain of command must coordinate the interrogation plan with the detention operations commander. Close coordination must occur between intelligence personnel and personnel responsible for detainee operations, including MP, security forces, Master at Arms, and other individuals providing security for detainees (hereafter referred to as guards). Guards do not conduct intelligence interrogations and, in accordance with DOD Directive 3115.09, will not set the conditions for interrogations. Guards may support interrogators as requested for detainee custody, control, escort, and/or additional security (for example, for combative detainees), in accordance with paragraphs 5-57 through 5-66 and FM 3-19.40, JP 3-63, and the approved interrogation plan.

M-12. The detention operations commander (in conjunction with the MI commander) may convene a multidiscipline custody and control oversight team including, but not limited to, MP, MI, BSC (if available), and legal representatives. The team can advise and provide measures to ensure effective custody and control in compliance with applicable law and policy.

M-13. Commanders must consider the following when employing separation:

- Is separation directed against the appropriate individual and is it necessary for collecting important intelligence?
- Does separation complement the overall interrogation strategy and interrogation approach technique or techniques?
- Is the application of separation with the specific detainee at issue consistent with humane treatment and in accordance with applicable law and policy?

M-14. Planning for the use of separation requires coordination with staff elements that provide support to interrogation operations. Staff elements that support interrogation facilities and forces employing separation will comply with paragraphs 4-59 and 4-60 and all controls and safeguards identified in paragraphs M-17 through M-26.

GENERAL CONTROLS AND SAFEGUARDS

HUMANE TREATMENT

M-15. All captured or detained personnel shall be treated humanely at all times and in accordance with DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, “Department of Defense Detainee Program,” and no person in the custody or under the control of the DOD, regardless of nationality or physical location, shall be subject to cruel, inhuman, or degrading treatment or punishment as defined in US law, including the

Detainee Treatment Act of 2005. All intelligence interrogations, debriefings, or tactical questioning to gain intelligence from captured or detained personnel shall be conducted in accordance with applicable law and policy.

M-16. Any inhumane treatment—including abusive practices, torture, or cruel, inhuman, or degrading treatment or punishment as defined in US law, including the Detainee Treatment Act of 2005—is prohibited and all instances of such treatment will be reported immediately in accordance with paragraph 5-69 thru 5-72. Beyond being impermissible, these unlawful and unauthorized forms of treatment are unproductive because they may yield unreliable results, damage subsequent collection efforts, and result in extremely negative consequences at national and international levels. Review by the servicing SJA is required prior to using separation. Each interrogation plan must include specific safeguards to be followed: limits on duration, interval between applications, and termination criteria. Medical personnel will be available to respond in the event a medical emergency occurs.

FM 2-22.3 REQUIREMENTS

M-17. Separation must be employed in accordance with the standards in this manual. These standards include the following:

- Prohibitions against abusive and unlawful actions (see para 5-75) and against the employment of military working dogs in the conduct of interrogation (see paras 5-59 and 8-2).
- Requirement for non-DOD agencies to observe the same standards for the conduct of interrogation operations and treatment of detainees when in DOD facilities (see para 5-55).
- Prohibition on guards conducting intelligence interrogations or taking any actions to set the conditions for interrogations. Humane treatment, evacuation, custody and control (reception, processing, administration, internment, and safety) of detainees; force protection; and the operation of the internment facility are discussed in paragraphs 5-57 through 5-66. (FM 3-19 .40 and JP 3-63 also thoroughly discuss detainee operations.)
- Assignment of ISNs to all detainees in DOD control, whether or not interrogation has commenced, as soon as possible; normally within 14 days of capture. (See AR 190-8 and Secretary of Defense Memorandum dated 20 September 2005, "(S//NF) Policy on Assigning Detainee Internment Serial Numbers (ISN)(U)."
- Access to detainees by the ICRC.

REPORTING OF ABUSES AND SUSPECTED ABUSES

M-18. As an interrogation technique, separation is particularly sensitive due to the possibility that it could be perceived as an impermissible act. Interrogators applying the separation technique and the chain of command supervising must be acutely sensitive to the application of the technique to ensure that the line between permissible or lawful actions and impermissible or unlawful actions is distinct and maintained. Therefore, HUMINT collectors should have heightened awareness and understanding of the risks,

control measures, and safeguards associated with the use of separation. Any interrogation technique that appears to be cruel, inhuman, or degrading as defined in US law; or impermissibly coercive, or is not listed in this manual, is prohibited and should be reported immediately to the chain of command or other appropriate channels for resolution. Orders given to treat detainees inhumanely are unlawful. Every interrogator must know how to respond to orders that the individual interrogator perceives to be unlawful (see paras 5-80 through 5-82).

M-19. If the order is a lawful order, it should be obeyed. Failure to obey a lawful order is an offense under the UCMJ.

COMMAND POLICY AND OPERATION ORDERS

M-20. The provisions of this appendix must be written into COCOM policy and/or OPORDs when using the restricted interrogation technique of separation.

MEDICAL

M-21. Commanders are responsible to ensure that detainees undergoing separation during interrogation receive adequate health care as described in greater detail in paragraph 5-91.

TRAINING AND CERTIFICATION

M-22. Only those DOD interrogators who have been trained and certified by the United States Army Intelligence Center (USAIC), or other Defense HUMINT Management Office (DHMO) designated agency, in accordance with guidance established by USD(I) to use separation, are authorized to employ this technique. The training must meet certification standards established by the Defense HUMINT Manager in coordination with applicable DOD components. Properly trained and certified contract interrogators are authorized to initiate interrogation plans that request the use separation, and, once the plan is approved, to employ the technique in accordance with the provisions of this appendix and Appendix K. Contract interrogators will always be utilized under the supervision and control of US government or military personnel (see para K-19 and K- 20). Non-DOD personnel conducting interrogations in DOD facilities must be certified by their agency and separately gain approval (through their agency's chain of command) for the additional technique described in this appendix. They must present this written certification and agency approval to the COCOM before use is permitted (see para 5-55).

PLANNING

M-23. Planning for the use of separation must include—

- An interrogation plan that addresses safeguards, limits of duration, interval between applications, termination criteria, and presence of qualified medical personnel for emergencies (see Figure M-2).
- A provision for detainees to be checked periodically in accordance with command health care directives, guidance, and SOPs applicable to all detainees.
- A legal review.

Page _____ of _____

INTERROGATION PLAN
FOR USE OF
RESTRICTED SEPARATION TECHNIQUE

THIS FORM IS TO BE COMPLETED IN CONJUNCTION WITH, AND MAINTAINED WITH, THE BASE INTERROGATION PLAN, FIGURE 10-3, FM 2-22.3. USE ADDITIONAL FORMS AS NEDED.

COCOM/SECDEF ORDER OR PLAN #:_____

RESTRICTED TECHNIQUE STRATEGY:

JUSTIFICATION:_____

USED IN CONJUNCTION WITH THE FOLLOWING APPROACH STRATEGIES:_____

SPECIFIC DESCRIPTION OF THE SEPARATION TECHNIQUE EMPLOYMENT STRATEGY:_____

PROPOSED DURATION:_____ REQUIRED BREAK:_____

SPECIFIC SAFEGUARDS AND OVERSIGHT TO BE EMPLOYED:

GUARDS:_____

INTERROGATORS:_____

OTHER:_____

DOCUMENTATION OF USE: (PHOTOS, VIDEO, NOTES)_____

TERMINATION CRITERIA TECHNIQUE:_____

REVIEW: Interrogation Supervisor:_____ MI Unit Cdr:_____ GO/OF SJA_____

APPROVAL AUTHORITY:	PRINTED NAME	DTG OF APPROVAL
GENERAL OFFICER/FLAG OFFICER	_____	_____
APPROVED FOR _____		DURATION
MI UNIT COMMANDER	_____	_____
INTERROGATION SUPERVISOR	_____	_____

SAMPLE

Figure M-2. Installation Plan for Restricted Separation Techniques.

- Documentation of the use of separation, including photographs and/or videotaping, if appropriate and available (see para 5-54).

M-24. Separation is only authorized for use in interrogation operations, not for other Military Source Operations. Separation may be approved for use in combination with authorized approach techniques. General controls and safeguards contained in this manual must be applied during the use separation, in conjunction with the safeguards specific to the separation technique. **Planning must consider the possible cumulative effect of using multiple techniques and take into account the age, sex, and health of detainees, as appropriate.**

TECHNICAL CONTROL

M-25. Requests for approval of separation will be forwarded (for information purposes only) via secure means through intelligence technical channels at the same time as they are sent through command channels. Intelligence technical channels are those used for forwarding of source information and technical parameters of collection operations from lower to higher and passing tasking specifics, source information, technical control measures, and other sensitive information from higher to lower. The technical chain extends from the HCT through the OMT and Operations Section (if one exists) to the C/J/G/S2X.

APPLICATION OF SEPARATION TECHNIQUE

M-26. The purpose of separation is to deny the detainee the opportunity to communicate with other detainees in order to keep him from learning counter-resistance techniques or gathering new information to support a cover story, decreasing the detainee's resistance to interrogation. Separation does not constitute sensory deprivation, which is prohibited. For the purposes of this manual, sensory deprivation is defined as an arranged situation causing significant psychological distress due to a prolonged absence, or significant reduction, of the usual external stimuli and perceptual opportunities. Sensory deprivation may result in extreme anxiety, hallucinations, bizarre thoughts, depression, and anti-social behavior. Detainees will not be subjected to sensory deprivation.

M-27. Physical separation is the best and preferred method of separation. As a last resort, when physical separation of detainees is not feasible, goggles or blindfolds and earmuffs may be utilized as a field expedient method to generate a perception of separation.

M-28. Objectives:

- Physical Separation: Prevent the detainee from communicating with other detainees (which might increase the detainee's resistance to interrogation) and foster a feeling of futility.
- Field Expedient Separation: Prolong the shock of capture. Prevent the detainee from communicating with other detainees (which might increase the detainee's resistance to interrogation) and foster a feeling of futility.

M-29. Safeguards:

- **Duration:** Self-explanatory.
- **Physical Separation:** Limited to 30 days of initial duration.
- **Field Expedient Separation:** Limited to 12 hours of initial duration at the initial interrogation site. This limit on duration does not include the time that goggles or blindfolds and earmuffs are used on detainees for security purposes during transit and evacuation.
- **Oversight Considerations for Field Expedient Separation:**
 - The intended use of field expedient means of separation must be specified on the interrogation plan that is submitted to the GO/FO for approval.
 - Detainees must be protected from self-injury when field expedient means of separation are used. The effect of the application of field expedient separation means on the detainee must be monitored to detect any possible health concerns.

M-30. The following safeguards apply to both Physical Separation and Field Expedient Separation.

- **Break:** Additional periods of separation will not be applied without the approving GO/FO's determination of the length of a break between iterations.
- **Extension:**
 - **Physical Separation Method**: Extensions of this technique past 30 days must be reviewed by the servicing SJA and approved by the original approving GO/FO or his replacement in that position.
 - **Field Expedient Method:** Extensions past 12 hours of initial duration at the initial interrogation site must be reviewed by the servicing SJA and approved by the original approving/replacement GO/FO.
 - **Medical:** Detainees will be checked periodically in accordance with command health care directives, guidance, and SOPs applicable to all detainees.
 - **Custody and Control:** The interrogation chain of command must coordinate the interrogation plan with the Detention Operations Commander. The Detention Operations Commander (in conjunction with the MI commander) may convene a multidiscipline custody and control oversight team including, but not limited to, MP, MI, BSC (if available), and legal representatives. The team can advise and provide measures to ensure effective custody and control in compliance with the requirements of applicable law and policy.
- **Oversight Considerations:**
 - Use of hoods (sacks) over the head, or of duct tape or adhesive tape over the eyes, as a separation method is prohibited.
 - If separation has been approved, and the interrogator subsequently determines that there may be a problem, the interrogator should seek further guidance through the chain of command before applying the technique.

- Care should be taken to protect the detainee from exposure (in accordance with all appropriate standards addressing excessive or inadequate environmental conditions) to—
 - Excessive noise.
 - Excessive dampness.
 - Excessive or inadequate heat, light, or ventilation.
 - Inadequate bedding and blankets.
 - Interrogation activity leadership will periodically monitor the application of this technique.
- Use of separation must not preclude the detainee getting four hours of continuous sleep every 24 hours.
- Oversight should account for moving a detainee from one environment to another (thus a different location) or arrangements to modify the environment within the same location in accordance with the approved interrogation plan.

M-31. Suggested Approach Combinations:

- Futility.
- Incentive.
- Fear Up.

Glossary

The glossary lists acronyms and terms with Army or joint definitions, and other selected terms. Where Army and joint definitions are different, (*Army*) follows the term. Terms for which FM 2-22.3 is the proponent manual (the authority) are marked with an asterisk (*) and followed by the number of the paragraph (¶) or page where they are defined. For other terms, refer to the manual listed. JP 1-02, Dictionary of Military and Associated Terms and FM 1-02 Operational Terms and Graphics are posted on the Joint Electronic Library, which is available online and on CD ROM.

- Use this URL to access JP 1-02 online: http://atiam.train.army.mil/soldierPortal/atia/adlsc/view/public/11444-1/FM/1-02/TOC.HTM
- Use this URL to access FM 1-02 online: http://atiam.train.army.mil/soldierPortal/atia/adlsc/view/public/11444-1/FM/1-02/TOC.HTM
- /jel/service_pubs/101_5_1.pdf
- Follow this path to access JP 1-02 on the Joint Electronic Library CD-ROM: Mainmenu>Joint Electronic Library>DOD Dictionary.
- Follow this path to access FM 1-02 on the Joint Electronic Library CD-ROM: Mainmenu>Joint Electronic Library>Service Publications>Multiservice Pubs> FM 101-5-1.

*2X	The *2X Staff conducts mission and RM for all HUMINT and CI entities located within the designated AOIR. It coordinates, deconflicts, and synchronizes all HUMINT and CI activities in the designated AOIR. ("*2X" indicates 2X functions at all levels.)
AC	Active Component
ACCO	Army Central Control Office
ACE	analysis and control element
ACT	Analysis Control Team
ADA	Air Defense Artillery
ADP	automated data processing
ADCON	administrative control
aka	also known as
AMHS	Automated Message Handling System
AMID	allied military intelligence battalion
AO	area of operations
AOI	area of interest
AOIR	area of intelligence responsibility
AOR	area of responsibility

approx	approximately
ARNG	Army Reserve National Guard
ASAS	All-Source Analysis System
ASCC	Army Service Component Command
ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
ASI	additional skill identifier
assn	assassination
ATD	associated technical document
BAT	Biometric Automated Toolset
BCT	brigade combat team
BDA	battle damage assessment
BOS	Battlefield Operating System
BSC	Behavioral Science Consultant
BSD	basic source data
C2	command and control
CA	civil affairs
CAT	category
CCIR	commander's critical information requirement
CCNY	City College of New York
CDOC	captured document
CDR	commander
CGS	common ground station
CE	captured equipment (STANAG term)
CED	captured enemy document
CEE	captured enemy equipment
CENTCOM	US Central Command
CFSO	Counterintelligence Force Protection Source Operations
CHAMS	CI/HUMINT Automated Management System
CHATS	CI/HUMINT Automated Tool Set
CI	counterintelligence
CIA	Central Intelligence Agency
CICA	Counterintelligence Coordination Authority
CIAC	Counterintelligence Analysis Cell

CID	Criminal Investigation Division
CIFA	Counterintelligence Field Agency
C2X	Coalition Intelligence Staff Officer
C/J2X LNO	Coalition/Joint Intelligence Staff Liaison Officer
C/J/G2X	Coalition/Joint/Corps/Division Intelligence Staff Officer
C/J/G/S2	Coalition/Joint/Corps/Division/Brigade and Below Intelligence Staff Officer
C/J/G/S2X	Coalition/Joint/Corps/Division/Brigade and Below Intelligence Staff Officer
CMO	civil-military operations
COA	course of action
COCOM	Combatant Command
COE	common operating environment
COLISEUM	Community On-Line Intelligence System for End Users and Managers
COMMZ	communications zone
CONUS	continental United States
CONOP	contingency operations
COP	common operational picture
COR	contracting officer representative
COT	commercial off-the-shelf
COTR	Contracting Officer's Technical Representative
counterintelligence	Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (FM 2-0)
Counterintelligence Coordinating Authority	Subordinate to the J/G2X and coordinates all CI activities for a deployed force. It provides technical support to all CI assets and coordinates and deconflicts CI activities in the deployed AO. (FM 2-0)
CP	command post
CPERS	captured personnel (JP-2.5)
CPR	Common Point of Reference
CS	combat support
CSS	combat service support
CTF	coalition task force

DA	Department of the Army
DCGS-A	Distributed Common Ground System-Army
DCIS	Defense Criminal Investigative Service
DCISS	Defense Intelligence Agency CI Information System
DCP	detainee collection point
DEA	Drug Enforcement Agency
debriefing	The systematic questioning of individuals to procure information to answer specific collection requirements by direct and indirect questioning techniques. (FM 2-0)
DED	Data Element Dictionary
DH	Defense HUMINT
DHMO	Defense HUMINT Management Office
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DII	DOD Information Infrastructure
DISCOM	Division Support Command
DOCEX	document exploitation
document exploitation	The systematic extraction of information from all media formats in response to collection requirements. (FM 2-0)
DOD	Department of Defense
DOE	Department of Energy
DP	displaced person
DRP	Detainee Reporting
DRS	Detainee Report System
DS	direct support
DSCA	defense support of civilian authorities
DSS	decision support software
DST	decision support template
DTG	date-time group
EAC	echelons above corps
EEFI	essential elements of friendly information
EPW	enemy prisoner of war
evaluating	In intelligence usage, appraisal of an item of information in terms of credibility, reliability, pertinence, and accuracy. (FM 2-0)

EW	electronic warfare
FBI	Federal Bureau of Investigation
FEO	forced entry operations
FFIR	friendly force information requirement
FHA	foreign humanitarian assistance
FISS	Foreign Intelligence Security Service
Five S's	search, seize, segregate, safeguard, and silence
FORSCOM	US Army Forces Command
FRAGO	fragmentary order
FRN	field reporting number
FSE	fire support element
Gb	gigabyte
GC	Geneva Convention Relative to the Protection of Civilian Persons in Time of War
GPS	Global Positioning System
GPW	Geneva Convention Relative to the Treatment of Prisoners of War
GRCS	Guardrail Common Sensor
GRIFN	Guardrail Information Node
GS	general support
GSR	general support-reinforcing
GUI	graphic user interface
GWS	Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field
HAC	HUMINT analysis cell
HAT	HUMINT analysis team
HCR	HUMINT collection requirement
HCT	HUMINT collection team
HET	human exploitation team
HN	host nation
HOC	HUMINT operations cell
HSOC	Homeland Security Operations Center
HQ	headquarters
HQDA	Headquarters, Department of the Army

human intelligence	The collection by a trained HUMINT collector of foreign information from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, and capabilities. (FM 2-0)
HUMINT	Human Intelligence
HUMINT Analysis Cell	The "fusion point" for all HUMINT reporting and operational analysis in the ACE and JISE. It determines gaps in reporting and coordinates with the requirements manager to cross-cue other intelligence sensor systems.
HUMINT Analysis Team	Sub-element of the G2 ACE that supports the G2 development of IPB products and developing and tailoring requirements to match HUMINT collection capabilities.
HUMINT Operations Cell	Assigned under the J/G2X to track all HUMINT activities in the area of intelligence responsibility (AOIR). It provides technical support to all HUMINT collection operations and deconflicts HUMINT collection operations in the AO. (FM 2-0)
I&WS	Deputy Under Secretary of Defense for Intelligence and Warfighting Support
IAFIS	Integrated Automated Fingerprint Identification System
IBS	Integrated Broadcast Services
ICF	intelligence contingency fund
ICRC	International Committee of the Red Cross
ID	identification
IED	improvised explosive device
IG	Inspector General
IIMG	Interagency Incident Management Group
IIR	intelligence information report
IMINT	imagery intelligence
INTREP	intelligence report
INTSUM	intelligence summary
IPB	intelligence preparation of the battlefield
IPF	Intelligence Processing Facility
IPSP	Intelligence Priorities for Strategic Planning
IR	information requirements
ISA	International Standardization Agreement
ISN	Internment Serial Number
ISR	intelligence, surveillance, and reconnaissance
IU	Interrogation Unit (AJP-2.5)

J2	Joint Intelligence Directorate/Staff
J2X	Joint Intelligence Staff Officer
J2X	Responsible for controlling, coordinating and deconflicting all HUMINT and CI collection activities and keeping the joint force J2 informed on all HUMINT and CI activities conducted in the joint force AOR. (*2X Staff Handbook) Umbrella organization consisting of human intelligence operation cell and the task force counterintelligence coordinating authority. The J2X is responsible for coordination and deconfliction of all human source-related activity. See also counterintelligence; human intelligence. (JP 2-01)
J5	Joint Staff Directorate, Civil Affairs
J/G2	Joint/Corps/Division Intelligence Staff Officer
J/G/S2	Joint/Corps/Division/Brigade and Below Intelligence Staff Officer
J/G/S2X	Joint/Corps/Division/Brigade and Below Intelligence Staff Officer
JAC	Joint Analysis Center
JAO	joint area of operations
JCMEC	Joint Captured Materiel Exploitation Center
JDEF	joint document exploitation facility
JDS	Joint Dissemination System
JFC	Joint Forces Commander
JIC	Joint Interrogation Center
JIDC	Joint Interrogation and Debriefing Center
JISE	Joint Intelligence Support Element
JTF	joint task force
JUMPS	job, unit, mission, PIR and IR, and supporting information
JWICS	Joint Worldwide Intelligence Communications System
KB	knowledgeability brief
LCC	Land Component Command
LDR	Lead Development Report
LEA	law enforcement agency
LNO	Liaison Officer
LRS	long-range surveillance
LTIOV	latest time information is of value
MAGTF	Marine Air-Ground Task Force
MASINT	measurement and signature intelligence
MDMP	Military Decisionmaking Process

MEDEVAC	medical evacuation
MEF	Marine expeditionary force
MEJA	Military Extraterritorial Jurisdiction Act
METT-TC	mission, equipment, terrain and weather, troops and support available, time available, and civil considerations
MI	Military Intelligence
MILO	mission, identification, location, and organization
MSO	military source operations
MOS	military occupation specialty
MP	Military Police
MTOE	modified table of organization and equipment
MTW	major theater war
NA	not applicable
NAC	national agency check
NAI	named area of interest
NATO	North Atlantic Treaty Organization
NBC	nuclear, biological, and chemical
NCO	noncommissioned officer
NCOIC	noncommissioned officer in charge
NGA	National Geospatial-Intelligence Agency
NGO	non-governmental organization
NIP	Notice of Intelligence Potential
NIST	national intelligence support team
NOFORN	no foreign dissemination
NRT	near-real time
NSA	National Security Agency
NVG	night vision goggles
OB	order of battle
OCONUS	outside continental United States
OCR	optical character recognition
OGA	other government agencies
O/I	operations and intelligence
OIC	officer in charge
OMT	operational management team

OPCON	operational control
OPLAN	operations plan
OPORD	operations order
OSC	operations support cell
OSD	Office of the Secretary of Defense
OSINT	open-source intelligence
OPTEMPO	operational tempo
OVOP	overt operational proposal
PDA	Personal Digital Assistant
PIR	priority intelligence requirement
PME	peacetime military engagement
PMO	Provost Marshal Office
POL	petroleum, oils, and lubricants
POW	prisoner of war
PRETECHREP	preliminary technical report
priority intelligence requirements	Those intelligence requirements for which a commander has an anticipated and stated priority in the task of planning and decisionmaking. (JP 1-02)
PSO	peacetime stability operation (STANAG term)
PSYOP	Psychological Operations
PVO	private volunteer organization
PW	Prisoner of War (as used in the GPW)
R	reinforcing
R&S	reconnaissance and surveillance
RC	Reserve Components
RFI	request for information
RM	requirements management
ROE	rules of engagement
RSR	Resource Status Report
SALUTE	Size, Activity, Location, Unit, Time, Equipment
SBI	special background investigation
SCC	Service Component Commands
SCI	sensitive compartmented information
SCO	Sub-Control Office
SDR	Source-Directed Requirement

security detainee	Those detainees who are not combatants, but who may be under investigation or pose a threat to US forces if released.
SE	southeast
SECDEF	Secretary of Defense
SERE	survival, evasion, resistance, and escape
S.F.P.	Students for Peace
SIGINT	signals intelligence
SII	statement of intelligence interest
SIO	senior intelligence officer
SIPRNET	Secret Internet Protocol Router Network
SIR	specific information requirement
SITMAP	situation map
SJA	Staff Judge Advocate
SME	subject matter expert
SOF	Special Operations Forces
SOFA	Status of Forces Agreement
SOI	signal operating instruction
SOP	standing operating procedure
SOW	statement of work
Source (DOD)	1. A person, thing, or activity from which information is obtained. 2. In clandestine activities, a person (agent), normally a foreign national, in the employ of an intelligence activity for intelligence purposes. 3. In interrogation activities, any person who furnishes information, either with or without the knowledge that the information is being used for intelligence purposes. In this context, a controlled source is in the employment or under the control of the intelligence activity and knows that the information is to be used for intelligence purposes. An uncontrolled source is a voluntary contributor of information and may or may not know that the information is to be used for intelligence purposes. See also agent; collection agency. (JP 1-02)
SQL	structured query language
SSC	small-scale contingency
Stability and Reconstruction Operations	Those operations that sustain and exploit security and control over areas, populations, and resources. They employ military capabilities to reconstruct or establish services and support civilian agencies. Stability and reconstruction operations involve both coercive and cooperative actions.
STANAG	Standardization Agreement

TACON	tactical control
tactical questioning	The expedient initial questioning for information of immediate tactical value. Soldiers conduct tactical questioning based on the unit's SOP, ROE, and the order for that mission. Unit leaders must include specific guidance for tactical questioning in the order for appropriate missions. The unit S3 and S2 must also provide specific guidance down to the unit level to help guide tactical questioning. (FM 2-0)
TCICA	Theater Counterintelligence Coordination Authority
TCP	traffic control point
TDA	table of distribution and allowances
TDRC	Theater Detainee Reporting Center
TECHDOC	technical document
TECHNINT	technical intelligence
TES	Tactical Exploitation System
TF	task force
THREATCON	threat condition
TOE	table of organization and equipment
TPFDDL	Time-Phased Forces Deployment Data List
TTP	tactics, techniques, and procedures
TS	Top Secret
tvl	travel
TWS	Trusted Workstation
UCMJ	Uniform Code of Military Justice
UNCLASS	unclassified
unk	unknown
USAR	US Army Reserve
USB	Universal Serial Bus
USCENTCOM	US Central Command
USD(I)	Under Secretary of Defense for Intelligence
UTM	universal transverse mercator (grid)
UW	unconventional warfare
WARNO	warning order
WMD	weapons of mass destruction
WO	warrant officer
WTC	World Trade Center

This page intentionally left blank.

Bibliography

The bibliography lists field manuals by new number followed by old number, as indicated.

DOCUMENTS NEEDED

These documents must be available to the intended users of this publication.

JP 0-2. *Unified Action Armed Forces.* 10 July 2001.

JP 2-0. *Doctrine for Intelligence Support to Joint* Operations. 9 March 2000.

JP 2-01.2. *(U) Joint Doctrine and Tactics, Techniques, and Procedures for Counterintelligence Support to Operations (S//NF).* 13 June 2006.

JP 3-0. *Doctrine for Joint Operations*. 10 September 2001.

JP 3-63. *Joint Doctrine for Detainee Operations.* September 2005.

JP 4-0. *Doctrine for Logistic Support of Joint Operations*. 6 April 2000.

AR 40-25. *Nutrition Standards and Education.* 15 June 2001.

AR 715-9. *Contractors Accompanying the Force*. 29 October 1999.

DA Pam 715-16. *Contractor Deployment Guide.* 27 February 1998.

FM 1. *The Army.* 14 June 2005.

FM 1-02. *Operational Terms and Graphics.* 21 September 2004.

FM 2-0. *Intelligence.* 17 May 2004.

FM 3-0. *Operations*. 14 June 2001.

FM 3-100.21. *Contractors on the Battlefield*. 3 January 2003.

FM 5-0. *Army Planning and Orders Production.* 20 January 2005.

FM 6-0. *Mission Command: Command and Control of Army Forces.* 11 August 2003.

FM 27-10. *Law of Land Warfare.* July 1956.

FM 34-5. (U) *Human Intelligence and Related Counterintelligence Operations* (S//NF). 29 July 1994.

FM 34-130. *Intelligence Preparation of the Battlefield*. 8 July 1994.

FM 63-11. *Logistics Support Element Tactics, Techniques, and Procedures*. 8 October 1996.

FM 71-100. *Division Operations.* 28 August 1996.

FM 100-15. *Corps Operations.* 13 September 1989.

FM 101-5. *Staff Organization and Operations*. 31 May 1997.

AMC Pam 715-18. *AMC Contracts and Contractors Supporting Military Operations*. June 2000.

READINGS RECOMMENDED

These sources contain relevant supplemental information.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online:
http://155.217.58.58/atdls.htm

AR 190-8. *Enemy Prisoners of War, Retained Personnel, Civilian Internees and Other Detainees*. 1 October 1997.

AR 190-40. *Serious Incident Report.* 15 July 2005.

AR 195-5. *Criminal Investigation Evidence Procedures*. 28 August 1982.

AR 380-5. *Department of the Army Information Security Program*. September 2000.

AR 380-10. *Technology Transfer, Disclosure of Information, and Contacts with Foreign Representatives.* 15 February 2001.

AR 380-15. *(C) Safeguarding Classified NATO Information.* 1 March 1984.

AR 380-28. *Department of the Army Special Security System*. 12 December 1991.

AR 380-40. *Policy for Controlling and Safeguarding Communications Security (COMSEC) Material.* 22 October 1990.

AR 380-49. *Industrial Security*. 15 April 1982.

AR 380-53. *Telecommunications Security Monitoring*. 29 April 1998.

AR 380-67. *Personnel Security Program*. 9 September 1988.

AR 381-1. *Security Controls on Dissemination of Intelligence Information*. 12 February 1990.

AR 381-10. *US Army Intelligence Activities*. 1 July 1984.

AR 381-12. *Subversion and Espionage Directed Against the US Army (SAEDA).* 15 January 1993.

AR 381-14. *Technical Counterintelligence (TCI).* 30 September 2002.

AR 381-20. *(U) US Army Counterintelligence Activities (S).* 26 September 1986.

AR 381-45. *Investigative Records Repository*. 25 August 1989.

AR 381-47. *(U) US Army Offensive Counterespionage Activities (S).* 30 July 1990.

AR 381-100. *(U) Army Human Intelligence Collection Program (S//NF).* 15 May 1988.

AR 381-102. *(U) US Army Cover Support Program (S).* 10 January 1991.

AR 381-143. *Military Intelligence Nonstandard Material Polices and Procedures*. 1 December 1986.

AR 381-172. (U) *Counterintelligence Force Protection Operations (CFSO) and Low Level Source Operations (LLSO) (S//NF).* 30 December 1994.

AR 385-10. *The Army Safety Program*. 23 May 1988.

AR 614-115. *Military Intelligence Excepted Career Program*. 12 April 2004.

AR 614-200. *Military Intelligence Civilian Excepted Career Program*. 30 September 2004.

AR 715-9. *Contractors Accompanying the Force.* 29 October 1999.

DA Pam 381-15. *Foreign Military Intelligence Collection Activities Program.* 1 June 1988.

DA Pam 385-1. *Small Unit Safety Officer/NCO Guide*. 29 November 2001.

TRADOC Reg 25-36. *The TRADOC Doctrinal Literature Program (DLP).* 1 October 2004.

FM 2-0. *Intelligence.* 17 May 2004.

FM 3-19.4. *Military Police Leader's Handbook*. March 2002.

FM 3-19-40. *Military Police Internment/Resettlement Operations*. August 2001.

FM 4-02.21. *Division and Brigade Surgeon's Handbook of Tactics, Techniques and Procedures*. November 2000.

FM 5-0. *Staff Organizations and Operations.* 31 May 1997.

FM 19-4. *Military Police Battlefield Circulation Control, Area Security, and Enemy Prisoner of War Operations.* 7 May 1993.

FM 27-10. *Law of Land Warfare*. July 1956.

FM 34-3. *Intelligence Analysis*. March 1990.

FM 34-7-1. *Tactical Human Intelligence and Counterintelligence Operations.* April 2002.

FM 34-8. *Combat Commander's Handbook for Intelligence*. September 1992.

FM 34-54. *Technical Intelligence*. January 1998.

FM 34-60. *Counterintelligence*. 3 October 1995.

FM 41-10. *Civil Affairs Operations*. 11 January 1993.

FMI 3-19.40. *Military Police Internment/Resettlement Operations.* 30 September 2005.

TC 25-20. *A Leader's Guide to After-Action Reviews.* 30 September 1993.

ST 2-22.7. *Tactical Human Intelligence and Counterintelligence Operations.* April 2002.

ST 2-33.5. *US Army Intelligence Reach Operations.* 1 June 2001.

ST 2-50. *Intelligence and Electronic Warfare Assets.* June 2002.

ST 2-91.6. *Small Unit Support to Intelligence.* March 2004.

OTHER PUBLICATIONS

JP 2-01. *Joint Intelligence Support to Military Operations*. November 1996.

AR 350-1. *Army Training and Education*. 9 April 2003.

DIAM 58-11. (U*) DOD HUMINT Policies and Procedures (S//NF).* August 1993.

DIAM 58-12. *(U) DOD HUMINT Management Systems (S//NF).* June 1997.

AJP-2.5. *Handling of Captured Personnel, Materiel, and Documents*. September 2001.

DOD Directive 2310.1. *DOD Program for Enemy Prisoners of War (POW) and Other Detainees (Short Title: DOD Enemy POW Detainee Program).* 18 August 1994.

DOD Directive 2310.1E. *The Department of Defense Detainee Program*.

DOD Directive 3115.09. *DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning.* 3 November 2005.

DOD Directive 5100.77. *DOD Law of War Program.* 9 December 1998.

DOD Directive 5240.1. *DOD Intelligence Activities.* 3 December 1982.

DOD Directive 5525.5. *DOD Cooperation with Civilian Law Enforcement Officials.* 15 January 1986.

DOD Instruction 3020.41. *Contractor Personnel Authorized to Accompany the U.S. Armed Forces.* 3 October 2005

DOD Regulation 5200.1-R. *Information Security Program,* 1977.

DOD Regulation 5240.0-R. *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons.* December 1982.

DOD SOP for Collecting and Processing Detainee Biometric Data. 11 February 05

Protocol 1 Additional to the Geneva Conventions. *Part IV: Civilian Population, Section 1: General Protection Against Effects of Hostilities*. 1977.

Executive Order 12333, *United States Intelligence Activities*. 4 December 1981.

Under Secretary of Defense for Intelligence (USD(I) Memorandum, "*Guidance for the Conduct and Oversight of Defense Human Intelligence (HUMINT) (U).*" 14 December 2004.

Implementing Instructions to the USD(I) Memorandum. "*Guidance for the Conduct and Oversight of Defense Human Intelligence (HUMINT) (U).*" 7 September 2004.

SECDEF Memorandum, *Policy on Assigning Detainee Serial Numbers (ISN) (*U). 20 September 2005.

18 U.S.C. *Posse Comitatus Act of 1878,* § 1385.

Homeland Security Act of 2002.

Detainee Treatment Act of 2005, Public Law No. 109-163, Title XIV.

DA Form 1132-R. *Prisoner's Personal Property List – Personal Deposit Fund (LRA).* April 1986.

DA Form 4137. *Evidence/Property Custody Document. July* 1976.

DA Form 4237-R. *Detainee Personal Record*. August 1995.

DD Form 2745. *Enemy Prisoner of War Capture Tag*. May 1996.

Standardization Agreements (STANAG):

STANAG 1059. *Distinguishing Letters for Geographic Entities for Use by NATO Armed Forces.* Edition 8. April 2003.

STANAG 2022. *Intelligence Reports.* 29 September 1988.

STANAG 2033. *Interrogation of Prisoners of War (PW).* Edition 6. December 1994.

STANAG 2044. *Procedures for Dealing with Prisoners of War (PW).* Edition 5. June 1994.

STANAG 2084. *Handling and Reporting of Captured Enemy Equipment and Documents.* June 1986.

This page intentionally left blank.

Index

Entries are by paragraph number

A

ACE. See analysis and control element.
AJP 2.5, Appendix E
AO. See area of operations.
Activities matrix, 12-23, Figure 12-3. See also Automation analysis tools.
Analysis and control element, 2-16
Analyst support, 9-30.
Analytical
 Support, 12-2
 Tools, 12-16
Approach, 1-10, 7-15, 8-1
 Phase, 8-4
 Rapport, 8-9
 Strategies, 8-77
 Debriefing, 8-82
 Elicitation, 8-86
 Interrogation, 8-77
 Techniques, 8-17
 Transitions, 8-73
Approaches
 Change of Scenery, 8-63
 Direct, 8-19
 Emotional, 8-23
 Establish Your Identity, 8-58
 False Flag, 8-69
 File and Dossier, 8-55
 Incentive, 8-21
 Mutt and Jeff, 8-65
 Rapid Fire, 8-60
 Repetition, 8-59
 Silent, 8-62
 We Know All, 8-53
Area Handbook, 7-4
Area of operations, 1-29
Assets, HUMINT Collection, 4-40
Association Matrix, 12-19, Figure 12-2
Audio recording, 9-29
Automation, 13-2
 Analysis tools, 13-13
 Requirements for collectors, 13-24
 Systems, 13-21, L-3
 Workstation requirements, 13-25

B

Basic Source Data Reports (BSD), 10-13
Battlefield Operating System (BOS), 1-1
BEST MAPS, 5-45
Biographic Intelligence, 5-45
Biometrics, 13-4

C

C2X, 2-4
CA. *See* Civil Affairs.
Capabilities, 1-31
Capture Rates, 5-90
Capture tag, Figure D-1
Captured document
 Handling, I-12
 Log, I-24, Figure I-3
 Transmittal sheet, I-19, Figure I-2
Captured equipment handling, D-21
Central Intelligence Agency, 3-24
Change of Scenery Approach, 8-63
Checkpoint Operations, 5-7, 5-36, 5-42
CIA. *See* Central Intelligence Agency.
CICA. *See* Counterintelligence Coordination Authority.
CID. *See* Criminal Investigation Division.
Civil Affairs (CA) Units, 4-47, 4-58
Cold leads, 9-22
Collect, 1-2
Collection
 Objectives, 7-2
 Priority, 4-45
 Requirements, 7-4
Combat Service Support Units, 4-58
Combatants, viii
 Lawful, 6-18
 Unlawful, 6-18
Command Debriefing Team, 2-13
Command Relationships, (HUMINT) 4-11
 Army, Table 4-2
 Joint, Table 4-3
Common points of reference, 9-39. *See also* Map tracking.
Communication requirements, 13-27, 13-30, L-7
Contact reports, 10-14
Continuous Contacts, 5-16
Contractor, 1-7, K-1
Control Questions, 9-10
Coordinates register, 12-41

Coordination with other units and operations, 5-42, 5-56, 5-102
Counterintelligence
Coordination Authority, 2-8
Functions, 1-7, Figure 1-2
Screening, 6-39, table 6-1
Courses of Action, 4-44
Criminal Investigation Division, 4-58, 4-60, 5-42
Cultural Awareness, 1-29, 8-4

D

DEA. *See* Drug Enforcement Agency.
Databases, 12-46, 13-18
Debriefing, 1-21
Debriefing Operations, 1-21, 5-30
Legal Guidelines, 5-33
Operational Considerations, 5-34
Deceit, 9-23, 9-25, 9-26
Defensive Operations, 3-7
Detainee, 5-26
Geneva Convention categories, 6-14
Security, 5-58, 5-78
Interrogation Operations, 1-20
Direct Approach, 8-19
Direct Questioning, 9-4
Document
Accountability, I-19
Associated with a source, I-51
Categories, I-27
Exploitation (DOCEX) Operations, 1-24, 4-51, E-12, I-1, I-11, I-48
Exploitation Team, 2-14
Evacuation, I-12
Handling, I-14
Screening, I-25
Tag, I-14
Translation, I-43
Transmittal, I-34
Drug Enforcement Agency, 4-58

E

EAC HUMINT, 3-22
Emotional Approach, 8-23
EPW
Serial number, 6-12, 6-13
Status, 6-14
Early Entry Operations. *See also* HUMINT operations.
HUMINT Support of, 3-6
Economic Intelligence, 5-45
Elicitation, 8-80
Establish Your Identity Approach, 8-58
Exploit dispositions, 9-43

F

False Flag, 8-69
Field Interrogations Operations, 5-95
File and Dossier Approach, 8-55
Fingerprint scanner, 13-4
Five S's, D-7
Forced Entry Operations. *See also* HUMINT operations.
HUMINT Support of , 3-5
Formal Contacts, 5-28
Friendly Force Debriefing Operations, 1-21, 5-39

G

G2X, 2-4
Geneva Conventions, 5-68, 5-72
Categories of detainees, 6-15
Excerpts, Appendix A

H

HCT, 2-11. *See also* HUMINT Collection Team.
As an Independent Patrol, 3-14
Integrated with other operations, 3-14
Restricted to Base Camp, 3-14
Hot leads, 9-21
Human Intelligence, 1-4,
Structure, 2-1
HUMINT, 1-4
Agencies, 3-24
Analysis, 12-1
Analysis Cell, 2-16
Asset Capabilities, 4-17, 4-26, 4-45
HUMINT Collection, 1-8, 5-1
Aids, 9-28
Constraints, 4-41
In a Hostile Environment, 3-21
In Permissive Environment, 3-19
In Semi-permissive Environment, 3-20
Phases, 1-8
Plan, 7-9
HUMINT Collection Team, 2-11
Allocation to maneuver units, 5-96
HUMINT Collector, 1-7
Traits, 1-28
HUMINT Command and Control, 4-9
HUMINT Contacts, 5-5
One Time Contact, 5-7
Continuous Contacts, 5-16
Formal Contact, 5-28
HUMINT Control Organizations, 2-3 through 2-14
HUMINT Collection and Related Activities, 1-14
HUMINT Methodology, 1-14, 1-18
HUMINT Mission Planning, 4-35, 4-44
HUMINT Operations, 1-23
Assessing, 4-8
Executing, 4-7
Planning, 4-3
Preparing, 4-5

HUMINT Organization, Figure 2-1
HUMINT Requirements Analysis, 4-18
HUMINT Requirements Management, 4-16
HUMINT Source, 1-6
Database, 2-9, 12-7
Collection Activities, 1-16
Selection, 12-45
HUMINT Structure, 2-1
HUMINT Tasks, 1-5
HUMINT Technical Control, 4-10

I

Imagery Intelligence, 4-57
Incentive Approach, 8-21
Information Dissemination, 4-32
INSCOM, 3-22
Intelligence Battlefield Operating System, 1-1
Intelligence Estimate, 7-4
Intelligence information reports, 10-6
Intelligence preparation of the battlefield, 12-3
Intelligence Process, 1-2, Figure 1-1
Intelligence Production, 4-31
Intelligence Reach, 7-5, 7-6
Interrogation, 1-20, 5-50
Of wounded detainees, 5-91
Priorities, Figure, 6-3
Prohibited techniques, 5-68, 5-74
Prohibition against use of force, 5-73
Serial number allocation, Appendix F
Interrogation Operations, 5-50
Field, 5-96
Joint, 5-100
Interpreter program, 11-28, 11-29, 11-30
Interpreter use, 11-2
Advantages, 11-2
Briefing, 11-18
Cautions, 11-4
Controlling and correcting, 11-24
Disadvantages, 11-3
Evaluating, 11-28
Methods, 11-6, 11-7
Placement, 11-21
Techniques, 11-16
Interpreters, 11-1, 11-26
Civilian, 11-15
Evaluating, 11-28
Military, 11-14
INTSUM, 7-4
Iris scanner, 13-6
ISR Plan (Integrated), 4-3, 4-27, 4-28
Updating, 4-34

J

J2X, 2-4
JIDC Analysis Section, 2-17
Joint HUMINT, 3-23, 5-91
Joint Interrogation and Debriefing Center (JIDC), 5-102
Joint interrogation operations, 5-99

K

Knowledgeability Brief, 10-15

L

Lawful enemy combatants, 6-18
Lead development report, 10-15
Leads, 9-20
Levels of Employment, 3-14
Liaison Operations, 1-22, 5-46
Link analysis diagram, 12-16, 12-25, Figure 12-4
Limitations, 1-32
Local civilian debriefing operations, 1-21
Long-Range Surveillance, 5-42

M

Machine translation, 13-8
Maneuver unit support, 4-9
Map tracking, 9-35
Matrices, 12-18
Measurement and Signals Intelligence (MASINT), 4-57
Military geographic intelligence, 5-46
Military Intelligence Organizations, 4-57
Military Police in Association with Interrogation Operations, 5-56, Figure 6-2
Internment/resettlement operations, 6-14, Figure 6-2
Units, 4-58, 5-42
Mutt and Jeff, 8-65

N

National level intelligence agencies, 3-24
Notice of intelligence potential, 10-15

O

OB Factors, 12-43
Offensive Operations, 3-2
One-Time Contact, 5-7
Open source documents, I-10
Operational analysis and assessment, 12-8
Operational Coordination, 4-9
Operational Management Team (OMT), 2-10
Team leader requirements, 13-23
Operational reports, 10-4
Operations Orders, 4-53
Operations Plans, 4-54
Operations Support Cell, 2-7
Orders
Illegal, 5-80, 5-82
Organizational Chart, 9-28, Figure 2-1

P

Pattern analysis, 12-40, 12-42
Plan, 1-2
Planning and Preparation, 1-9, 7-1
Political intelligence, 5-45
Polygraph, 13-7
Detainee status, 6-14 through 6-23, E-8
Pre-deployment planning, Appendix C
Prepare, 1-2
Primary approach strategy, 7-15
Process, 1-2
Produce, 1-2
Protected persons, 6-17
Protocol I Additional to the Geneva Conventions, Appendix B
Psychological Operations (PSYOP) Units, 4-58, 5-42

Q

Questioning, 1-11
 Illiterates, 9-46
 Plan, 7-18
 Principles, 9-2
 Quick reference guide, Appendix G
 Sequence, 7-19, 7-20
Questions, 9-2
 Direct, 9-4
 Follow Up, 9-7
 Non-pertinent, 9-8
 Prepared, 9-12
 Repeat, 9-9
 To avoid, 9-14

R

Rapid Fire Approach, 8-60
Reach. *See* Intelligence Reach.
Recording principles and techniques, 9-29
References, Appendix J
Refugee debriefing operations, 1-21, 5-31
Repetition Approach, 8-59
Reporting, 1-13, 7-24, 10-1
 Channels, 10-3, 10-16, Figure 10-1
 Evaluation, 4-33
 Principles, 10-2
Report types, 10-3
Required areas of knowledge, 1-29
Research, 7-3
 Source-specific, 7-8, 7-25
Reserve component integration, 4-50
Restricted Interrogation Techniques, 8-71
Retained personnel, 6-22
Risk assessment, 4-43

S

S2 Guide for Handling Detainees, Appendix D
S2X, 2-4
SALUTE reports, 10-10
 Format, Appendix H
Science and technical intelligence, 5-45
Screening, 1-18, 6-1
 Codes, Table 6-1
 Community, 6-38
 Documents, I-25
 Local employees, 6-37
 Methodologies, 6-9
 MP support, 6-14, Figure 6-2
 Observations, 6-30
 Operations, 1-19, 6-7, 6-8
 Prisoner of war and refugee, 6-9 , 6-13
 Reports, 10-15
 Requirements, 6-7
 Sheet, Figure 6-1
Search engine, 13-14
Separation, M-1
Signals Intelligence, 4-57
Silent Approach, 8-62
Single-discipline HUMINT analysis and production, 12-14
Situation Map (SITMAP), 7-4
Sociological Intelligence, 5-45
SOF. *See* Special operation forces.
SOR development, 12-5
Source, 1-6
 Administrative reports, 10-5
 Analysis, 12-11
 Assessment, 6-36
 Coverage overlay, 12-50
 Map reading skills, 9-38
 Profiles, 12-51
 Reliability matrix, B-1
Special Operation Forces, 5-42
Stability and reconstruction operations, 3-9
Staff coordination, 4-59
Strategic Debriefing Operations, 5-43
Subject matter expert (SME), 7-4
Support Operations, 3-15
Support Relationships (HUMINT), 4-13
 Direct Support, Table 4-2
 General Support, Table 4-2
Support Scheme Development, 4-27, 4-60

T

Tactical Debriefing Operations, 5-35
Tactical questioning, 1-17
Target Folder, 4-39, 12-47
Task Organization, 4-47
Taskings and Requests, 4-28
Technical expert support, 9-30
Technical intelligence (TECHINT), 4-57
 Screening requirements for, 6-42
 Support, 7-17
Termination, 1-12

Phase, 8-84
Report, 10-15
Third-party information, 9-33
Time Event Chart, 9-28, 12-17, Figure 12-1
Traits of a HUMINT Collector, 1-28
Translation machines, 13-8
Translators, I-47
Transportation and telecommunication intelligence, 5-45
Trusted Workstation (TWS), 13-3

U

Umbrella concept, 7-4
Unit Augmentation, 4-58
Unlawful enemy combatant, viii, 6-18
Urban Operations, 3-16

V

Video Recording, 9-29
Warning Order, 4-37

W

We Know All Approach, 8-53
Web-based reporting, 13-15
Wounded detainees
Interrogation of, 5-91, 9-45

This page intentionally left blank.

FM 2-22.3 (FM 34-52)
6 September 2006

I have approved FM 2-22.3 in accordance with DOD Directive 3115.09, DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning.

STEPHEN A. CAMBONE
Under Secretary of Defense
for Intelligence

By Order of the Secretary of the Army:

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

Official:

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army
0516001

DISTRIBUTION:

Regular Army, Army National Guard, and the Army Reserve: To be distributed in accordance with the initial distribution number (IDN) 111130, requirements for FM 2-22.3.

This page intentionally left blank.

PIN: 082535-000